RA Dr. Bijan Moini • GFF • Boyenstr. 41 • 10115 Berlin

An das
Bundesverfassungsgericht
Postfach 1771
76006 Karlsruhe
– nur per beA –

Rechtsanwalt Dr. Bijan Moini M.A.

Gesellschaft für Freiheitsrechte
Boyenstr. 41, 10115 Berlin

E-Mail: kontakt@bijanmoini.de
Tel.: +49 30 549 0810 14

Unser Zeichen: VB-01-25

Berlin, den 22. Juli 2025

Verfassungsbeschwerde

1. 1
2. 2
3. 3
4. 4
5. 5
6. 6
7. 7
8. 8

- Beschwerdeführer*innen -

Bevollmächtigter:
Rechtsanwalt Dr. Bijan Moini,
Gesellschaft für Freiheitsrechte, Boyenstr. 41, 10115 Berlin

Namens und in Vollmacht **(Anlagenkonvolut 1)** der Beschwerdeführer*innen erhebe ich

Verfassungsbeschwerde

gegen

1. Art. 61a Abs. 1 Satz 1-3, Abs. 4 Satz 1-5, Abs. 5 Nr. 1-3
2. Art. 61a Abs. 2 Satz 1 Nr. 1, Satz 2-5 i.V.m. Art. 61a Abs. 1 Satz 1, Abs. 3, Abs. 4 Satz 1-5, Abs. 5 Nr. 1-3
3. Art. 61a Abs. 2 Satz 1 Nr. 2, Satz 2-5 i.V.m. Art. 61a Abs. 1 Satz 1, Abs. 3, Abs. 4 Satz 1-5, Abs. 5 Nr. 1-3

des Gesetzes über die Aufgaben und Befugnisse der Bayerischen Polizei (BayPAG) in der Fassung der Bekanntmachung vom 14. September 1990 (GVBl. S. 397, BayRS 2012-1-1-I), zuletzt geändert durch § 1 des Gesetzes zur Änderung des Polizeiaufgabengesetzes und weiterer Rechtsvorschriften vom 23. Juli 2024 (GVBl. S. 247).

Gerügt wird die Verletzung der Grundrechte der Beschwerdeführer*innen aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1, Art. 10 Abs. 1, Art. 13 Abs. 1 und Art. 19 Abs. 4 GG.

Inhaltsübersicht

A. Vorbemerkung

Datenanalysesoftware findet immer breitere Verwendung in deutschen Polizeibehörden. Nach Hessen und Nordrhein-Westfalen setzt nun auch der Freistaat Bayern eine Variante der Software Gotham des US-Unternehmens Palantir als sogenannte „Verfahrensübergreifenden Recherche- und Analyseplattform“ (im Folgenden: „VeRA“) ein. Durch den Abschluss eines Rahmenvertrags können auch andere Bundesländer und der Bund leichter ohne eigenes Vergabeverfahren auf die Software zugreifen. Auf Basis einer verfassungswidrigen Rechtsgrundlage nutzt die bayerische Polizei „VeRA“ ohne ausreichende Kontrollsysteme unter anderem zum Schutz von bloßen Eigentums- und Vermögenswerten. Vor diesem Hintergrund wendet sich die vorliegende Verfassungsbeschwerde gegen die Regelung im Gesetz über die Aufgaben und Befugnisse der Bayerischen Polizei (BayPAG), die sie zum Einsatz dieser Software zur Gefahrenabwehr ermächtigt (Art. 61a BayPAG).

Vergleichbare Vorschriften des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG) und des Hamburgischen Gesetzes über die Datenverarbeitung der Polizei (HmbPolDVG) hat das angerufene Gericht in seinem Urteil vom 16. Februar 2023 – 1 BvR 1547/19 und 1 BvR 2634/20 zur automatisierten Datenanalyse (im Folgenden: „Datenanalyseurteil“) für teilweise verfassungswidrig erklärt. In dieser Entscheidung hat das angerufene Gericht verfassungsrechtliche Maßstäbe für die Zulässigkeit automatisierter Datenanalysen durch die Polizei festgelegt. Der bayerische Gesetzgeber hat diese Vorgaben bei Erlass seines Gesetzes nicht ausreichend beachtet. Gegen die Rechtsgrundlage in Nordrhein-Westfalen (Az. 1 BvR 1908/22) und die neu gefasste Norm in Hessen (Az. 1 BvR 1557/24) sind aus demselben Grund bereits Verfassungsbeschwerden anhängig.

Art. 61a BayPAG ermöglicht komplexe, nicht nachvollziehbare Datenanalysen und damit in allen Tatbestandsvarianten schwerwiegende Grundrechtseingriffe und verletzt das Allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG), das Fernmeldegeheimnis (Art. 10 Abs. 1 GG)

und die Unverletzlichkeit der Wohnung (Art. 13 GG) sowie das Gebot effektiven Rechtsschutzes (Art. 19 Abs. 4 GG).

Analysiert werden riesige Mengen auch sensibler Daten, beispielsweise aus heimlichen Überwachungsmaßnahmen. So können umfassende Sammlungen wie aus Vorgangsdatenbanken und Einsatzleitsystemen analysiert werden. Es ist auch möglich, weitere Daten händisch hinzuzufügen. In die Analyse fließen in erheblichem Umfang Daten von Menschen ein, die keinen Anlass für polizeiliche Maßnahmen bieten, zum Beispiel Zeug*innen, Anzeigeerstatter*innen und Opfer von Straftaten.

Das Gesetz schränkt auch nicht ausreichend bestimmt ein, mit welcher Methode die Datenanalysen erfolgen dürfen, sodass auch Persönlichkeitsprofile und komplexe Gefährlichkeitsbewertungen von Personen erstellt werden können. Hinzu kommt, dass der Einsatz von Künstlicher Intelligenz (im Folgenden: „KI“) und hochkomplexen Algorithmen nicht wirksam beschränkt wird. Das bedeutet, dass Analysefunktionen zur Anwendung kommen können, die zu nicht nachvollziehbaren Ergebnissen führen. Durch den Einsatz von „VeRA“ ist wegen der KI-Funktionen der zugrundeliegenden Software Gotham sogar davon auszugehen, dass es dazu kommt.

Diese Datenanalysen sind außerdem unter zu geringen Voraussetzungen zulässig. Für alle Tatbestandsvarianten sind die verfassungsrechtlichen Anforderungen an Eingriffsschwelle und zu schützende Rechtsgüter nicht gewahrt. Datenanalysen dürfen mithin aus zu geringem Anlass erfolgen. Dies gilt zunächst, weil Datenanalysen schon bei drohenden Gefahren und damit zu weit im Vorfeld ermöglicht werden (Art. 61a Abs. 1 Satz 1, Abs. 2 Satz 1 Nr. 1 BayPAG). Schon bei Anhaltspunkten für Vorbereitungshandlungen zu Straftaten dürfen Datenanalysen durchgeführt werden, ohne dass feststehen muss, welche Personen beteiligt sein sollen. Auch die Anknüpfung an die Begehungsgefahr von Straftaten aus dem Katalog nach § 100b Abs. 2 StPO (Art. 61a Abs. 2 Satz 1 Nr. 1 BayPAG) genügt nicht, da die Straftaten auch weniger gewichtige Rechtsgüter wie bloße Sachwerte schützen. Die bundesgesetzliche Norm wird darüber hinaus in unzulässi-

ger Weise dynamisch in Bezug genommen. Außerdem werden Datenanalysen schon zum Schutz nur weniger gewichtiger und zu unbestimmter Rechtsgüter zugelassen, insbesondere bei der Gefahr der Begehung von Eigentums- und Vermögensdelikten (Art. 61a Abs. 2 Satz 1 Nr. 2 BayPAG).

Schließlich sieht das Gesetz kein ausreichendes Kontrollkonzept vor, um die Rechtmäßigkeit der Datenanalysen gerade auch während des Analysebetriebs durch regelmäßige externe Kontrollen sicherzustellen. Auch fehlt es an Regelungen zum Schutz vor Fehlern und diskriminierenden Analysemechanismen und -ergebnissen. Die Gefahren von Missbrauch, Datenabflüssen und unberechtigten Datenzugriffen, die mit der Nutzung von Softwareanwendungen privater Anbieter*innen wie dem US-amerikanischen Palantir einhergehen, werden gesetzlich nicht hinreichend ausgeschlossen.

B. Gegenstand der Verfassungsbeschwerde

I. Erläuterung der angegriffenen Vorschrift

Art. 61a BayPAG wurde mit dem Gesetz zur Änderung des Polizeiaufgabengesetzes und weiterer Rechtsvorschriften vom 23. Juli 2024 (GVBl. S. 247) eingeführt und ist am 1. August 2024 in Kraft getreten.

Nach Art. 61a Abs. 1 Satz 1 BayPAG kann die Polizei zur Gewinnung neuer Erkenntnisse personenbezogene Daten aus verschiedenen eigenen automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, automatisiert zusammenführen und darauf bezogen weitere nach dem BayPAG oder besonderen Rechtsvorschriften erhobene personenbezogene Daten verarbeiten, soweit dies zur Abwehr einer mindestens drohenden Gefahr für die dort genannten Rechtsgüter erforderlich ist. Die Norm ermöglicht damit automatisierte Datenanalysen.

Im Rahmen der Maßnahmen sind gemäß Art. 61a Abs. 5 Nr. 1-3 BayPAG automatisierte Entscheidungsfindungen im Sinne von Art. 11 Richtlinie (EU) 2016/680 (im Folgenden: JI-Richtlinie), die eine nachteilige Rechtsfolge für die betroffene Person haben oder sie erheblich beeinträchtigen, sowie der Einsatz selbstlernender Systeme und der unmittelbare automatisierte Abgleich personenbezogener Daten aus der Allgemeinheit offenstehenden Netzwerken, unzulässig. Allerdings können Daten aus sozialen Medien gemäß Art. 61a Abs. 1 Satz 1 BayPAG händisch einbezogen werden,

> LT-Drs. 19/1557, S. 24.

Die Vorschrift umfasst drei Tatbestandsvarianten (Art. 61a Abs. 1 Satz 1 sowie Abs. 2 Satz 1 Nr. 1 und Nr. 2) mit unterschiedlichen Eingriffsschwellen. Die erste Tatbestandsvariante (Art. 61a Abs. 1 Satz 1 BayPAG) erlaubt die automatisierte Datenanalyse zur Abwehr einer mindestens drohenden Gefahr für die dort genannten gewichtigen Rechtsgüter. Die drohende Gefahr wird in Art. 11a Abs. 1 BayPAG legaldefiniert.

Die zweite Tatbestandsvariante (Art. 61a Abs. 2 Satz 1 Nr. 1 BayPAG) ermöglicht den Einsatz der automatisierten Datenanalyse zur Verhütung

oder Unterbindung von besonders schweren Straftaten nach § 100b Abs. 2 StPO, wenn aufgrund tatsächlicher Anhaltspunkte innerhalb eines übersehbaren Zeitraums mit weiteren gleichgelagerten Straftaten zu rechnen ist. Die dritte Tatbestandsvariante (Art. 61a Abs. 2 Satz 1 Nr. 2 BayPAG) knüpft ebenfalls an die Abwehr einer Gefahr oder drohenden Gefahr an, erweitert jedoch den Kreis der zu schützenden Rechtsgüter (Art. 61a Abs. 2 Satz 1 Nr. 2 lit a-d BayPAG).

Anders als bei der ersten Tatbestandsvariante in Absatz 1 beschränkt Art. 61a Abs. 3 BayPAG für die übrigen Varianten des Absatzes 2 die Art der Datenbestände, auf die die Polizei bei der automatisierten Datenanalyse zugreifen darf.

Die Verarbeitung von Daten, die aus einer Wohnraumüberwachung stammen, ist für die erste Tatbestandsvariante auf die Abwehr dringender Gefahren beschränkt (Art. 61a Abs. 1 Satz 2 BayPAG). Für die übrigen Tatbestandsvarianten ist sie ganz ausgeschlossen, ebenso wie die Verarbeitung bestimmter biometrischer Daten und solcher Daten, die aus einer Online-Durchsuchung stammen oder Audio- oder Videomaterial enthalten (Art. 61a Abs. 2 Satz 3, 4 BayPAG).

Die allgemeinen polizeidatenschutzrechtlichen Vorschriften zur Zweckbindung und -änderung in Art. 48 Abs. 1, 3, 4, Art. 53 Abs. 2 sowie Art. 54 Abs. 2 Satz 1 bleiben unberührt (Art. 61a Abs. 1 Satz 3, Abs. 2 Satz 2 BayPAG), anders als die Kennzeichnungsverpflichtung in Art. 48 Abs. 5 BayPAG.

Art. 61a Abs. 4 BayPAG enthält für alle Tatbestandsvarianten die Verpflichtung, dass nur geschultes Personal die Software nutzen darf, wobei die Zugriffsmöglichkeiten auf das erforderliche Maß beschränkt sein sollen und die Ergebnisanzeige auf mit den Suchparametern übereinstimmende Treffer beschränkt sein muss. Vorgeschrieben ist außerdem die Dokumentation des Vorliegens der Voraussetzungen der Maßnahmen sowie die Protokollierung des Vorgehens bei Maßnahmen. Datenanalysen nach Art. 61a

Abs. 2 BayPAG dürfen außerdem nur durch in Art. 36 Abs. 4 BayPAG genannte Polizeibeamt*innen angeordnet werden (Art. 61a Abs. 2 Satz 5 BayPAG).

II. Die Beschwerdeführer*innen

[…]

C. Zulässigkeit

Die Verfassungsbeschwerde ist zulässig

I. Beschwerdebefugnis

Die Beschwerdeführer*innen sind im Sinne von § 90 Abs. 1 Bundesverfassungsgerichtsgesetz (BVerfGG) beschwerdebefugt. Sie sind selbst, gegenwärtig und unmittelbar von den Regelungen betroffen.

1. Verfassungsrechtliche Rügen

Die Beschwerdeführer*innen rügen eine Verletzung ihres Rechts auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG aufgrund der Möglichkeit, von einer Maßnahme nach Art. 61a Abs. 1 oder 2 BayPAG betroffen zu sein (dazu **D.**). Daneben machen sie eine Verletzung ihres Fernmeldegeheimnisses aus Art. 10 Abs. 1 GG geltend, da jedenfalls gemäß Art. 61 Abs. 1 Satz 1 BayPAG auch Daten aus Telekommunikationsüberwachungen in die Datenauswertung einfließen können. Ebenfalls können so auch Daten aus Online-Durchsuchungen verarbeitet werden, sodass die Beschwerdeführer*innen auch eine Verletzung ihres Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (IT-Grundrecht, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) rügen. Einbezogen werden können außerdem Daten, die durch den Einsatz technischer Mittel in Wohnungen (Art. 61a Abs. 1 Satz 2 BayPAG) erhoben wurden, weshalb die Beschwerdeführer*innen auch einen Verstoß gegen das Grundrecht auf Unverletzlichkeit der Wohnung aus Art. 13 Abs. 1 GG rügen.

Die Beschwerdeführer*innen rügen außerdem verfassungsrechtliche Defizite im Kontrollkonzept. Sie sind daher auch in Art. 19 Abs. 4 GG betroffen, weil sich die entsprechenden Anforderungen aus dem jeweiligen Grundrecht in Verbindung mit Art. 19 Abs. 4 GG ergeben,

> vgl. BVerfGE 141, 220 (282 Rn. 134).

2. Eigene und gegenwärtige Betroffenheit

Die Beschwerdeführer*innen sind nach § 90 Abs. 1 BVerfGG selbst und gegenwärtig von Art. 61a BayPAG betroffen.

Für die Darlegung der unmittelbaren sowie der eigenen und gegenwärtigen Betroffenheit gelten bei einer Verfassungsbeschwerde gegen eine gesetzliche Ermächtigung zu heimlichen Überwachungsmaßnahmen besondere Anforderungen,

> BVerfG, Beschluss vom 8. Oktober 2024, 1 BvR 1743/16, 1 BvR 2539/16, Rn. 87 ff.; BVerfGE, 169, 332 (358 Rn. 59); 169, 130 (154 Rn. 36); 165, 1 (31 Rn. 41).

Zur Begründung der Möglichkeit eigener und gegenwärtiger Betroffenheit durch eine gesetzliche Ermächtigung zu heimlichen Überwachungsmaßnahmen, bei der die konkrete Beeinträchtigung zwar erst durch eine Vollziehung erfolgt, die Betroffenen in der Regel aber keine Kenntnis von Vollzugsakten erlangen, reicht es aus, wenn die Beschwerdeführer*innen darlegen, mit einiger Wahrscheinlichkeit durch auf den angegriffenen Rechtsnormen beruhende Maßnahmen in eigenen Grundrechten berührt zu werden,

> BVerfG, Beschluss vom 8. Oktober 2024, 1 BvR 1743/16, 1 BvR 2539/16, Rn. 89; BVerfGE, 169, 332 (359 Rn. 61) 169, 130 (154 Rn. 38); 165, 1 (31 Rn. 43); 163, 43 (73 Rn. 87); 155, 119 (160 Rn. 75).

Bei der automatisierten Datenanalyse nach Art. 61a BayPAG handelt es sich um eine heimliche Überwachungsmaßnahme, von der Betroffene in der Regel keine Kenntnis erlangen, sodass sie lediglich darlegen müssen,

mit einiger Wahrscheinlichkeit durch Art. 61a BayPAG in eigenen Grundrechten berührt zu werden.

Diese Wahrscheinlichkeit können die Beschwerdeführer*innen darlegen. Dabei sind folgende Betroffenheitskonstellationen denkbar: als Zielperson (dazu **a.**) oder als drittbetroffene Person, das heißt als Kontaktperson (**b.**), oder als vollkommen unbeteiligte Person aufgrund der Streubreite der Maßnahme, insbesondere aufgrund gespeicherter Daten der Beschwerdeführer*innen (**c.**).

a. Als Zielperson

In besonderem Maße betroffen sind Zielpersonen der Analyse.

Ein Vortrag, für sicherheitsgefährdende Aktivitäten verantwortlich zu sein, ist dabei ebenso wenig erforderlich wie die Darlegung, durch die sich Beschwerdeführer*innen selbst einer Straftat bezichtigen müssten,

> BVerfG, Beschluss vom 8. Oktober 2024, 1 BvR 1743/16, 1 BvR 2539/16, Rn. 89; BVerfGE, 169, 332 (359 Rn. 61); 169, 130 (154 Rn. 38); 165, 1 (31 Rn. 43); 155, 119 (160 Rn. 75); BVerfGE 130, 151 (176 f. Rn. 102).

Bei den Beschwerdeführer*innen zu 1 bis 8 besteht die hohe Wahrscheinlichkeit, dass sie als Zielpersonen Maßnahmen nach Art. 61a Abs. 1 bzw. Abs. 2 BayPAG ausgesetzt werden.

Dies ergibt sich insbesondere daraus, dass die Eingriffsschwelle durch die Einbeziehung von Vorfeldtatbeständen in Art. 61a Abs. 2 Satz 1 Nr. 1 BayPAG sowie durch die Verwendung des Begriffs der „drohenden Gefahr“ in Art. 61a Abs. 1 Satz 1 und Abs. 2 Satz 1 Nr. 2 BayPAG weit ins Vorfeld einer Gefahr verlagert werden (dazu **D.II.1.a.bb.bbb.**).

Sämtliche Beschwerdeführer*innen sind mit einiger Wahrscheinlichkeit als Zielpersonen unmittelbar von der automatisierten Anwendung zur Datenanalyse betroffen, da sie politisch beziehungsweise in der Fanszene aktiv sind und sie bereits in der Vergangenheit häufiger Ziel polizeilicher Maßnahmen waren, sodass mit einiger Wahrscheinlichkeit zu erwarten ist,

dass sie auch künftig Überwachungsmaßnahmen, wie Maßnahmen nach Art. 61a BayPAG, ausgesetzt sein werden.

[…]

b. Als Drittbetroffene

Für eine Betroffenheit der Beschwerdeführer*innen ist jedoch nicht erforderlich, dass die Beschwerdeführer*innen als Zielpersonen einer Maßnahme nach Art. 61a BayPAG ausgesetzt sind. Es ist vielmehr ausreichend, dass ihre eigenen Daten mit einiger Wahrscheinlichkeit in die Analyse einbezogen werden.

Die Verarbeitung gespeicherter Datenbestände mittels Datenanalyse oder -auswertung greift in das Grundrecht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG aller Personen ein, deren Daten bei diesem Vorgang personenbezogen Verwendung finden. Die weitere Nutzung früher erhobener Daten über den ursprünglichen Anlass hinaus begründet einen neuen Grundrechtseingriff, der verfassungsrechtlich einer eigenständigen Rechtfertigung nach dem Grundsatz der Zweckbindung bedarf,

BVerfGE 165, 363 (388 Rn. 50); 141, 220 (324 Rn. 277, 327 Rn. 285).

Betroffene müssen also selbst nicht unmittelbar Zielperson der Datenanalyse sein. Die Analyse kann sich nämlich nicht nur auf Daten der Zielperson beziehen, sondern auf sämtliche personenbezogenen Daten, die in eigenen automatisierten Verfahren der Polizei vorhanden sind, sowie auf weitere nach dem BayPAG oder anderen Rechtsvorschriften erhobenen Daten (Art. 61a Abs. 1 Satz 1 BayPAG). Auch Art. 61a Abs. 2 i.V.m. Abs. 3 BayPAG enthält zwar eine Beschränkung der einzubeziehenden Datenbestände, nicht aber eine Beschränkung auf Daten der Zielperson.

aa. Aufgrund der Streubreite der Maßnahme

Für die Wahrscheinlichkeit eigener Betroffenheit der Beschwerdeführer*innen spricht schon die große Streubreite des Art. 61a BayPAG. Eine

große Streubreite ist gegeben, wenn die Maßnahme nicht auf einen tatbestandlich eng umgrenzten Personenkreis zielt, insbesondere wenn sie auch Dritte in großer Zahl zufällig erfassen kann,

> BVerfG, Beschluss vom 8. Oktober 2024, 1 BvR 1743/16, 1 BvR 2539/16, Rn. 89; BVerfGE, 169, 130 (155 Rn. 39); 165, 1 (32 Rn. 44).

Von einer großen Streubreite ist bei Art. 61a BayPAG deshalb auszugehen, weil eine Vielzahl personenbezogener Daten Unbeteiligter, die nicht zwangsläufig Kontaktperson sind oder Anlass zur Überwachung gegeben haben, darunter insbesondere Daten aus der Vorgangsverwaltung, einbezogen werden (dazu ausführlich **D.I.2.a.aa.ccc.** und **D.I.2.b.aa.fff.**). Ausschlüsse bezüglich der Daten bestimmter Personen oder Personengruppen sieht die Norm nicht vor. Deshalb ist es wahrscheinlich, dass die Daten der Beschwerdeführer*innen – unabhängig von ihrem politischen Engagement oder vergangener Ermittlungsverfahren – mit einiger Wahrscheinlichkeit bereits jetzt oder künftig in Datenanalysen nach Art. 61a BayPAG einbezogen werden.

bb. Als Kontaktperson

Das angerufene Gericht erkennt in seiner Rechtsprechung an, dass auch eine Verbindung zu Zielpersonen – sei sie politisch, beruflich oder privat – eine eigene Betroffenheit ergeben kann. Nicht erforderlich ist dabei der Vortrag von Informationen, die von einem Zeugnisverweigerungsrecht etwa nach §§ 52, 53, 53a StPO umfasst sind,

> vgl. BVerfGE 169, 130 (155 Rn. 39)165, 1 (32 Rn. 44).

Bei Kontaktpersonen besteht eine gesteigerte Wahrscheinlichkeit, dass Daten als Beifang in die Datenbestände der Polizei und damit auch in eine automatisierte Datenanalyse nach Art. 61a BayPAG einfließen. Das kann etwa geschehen, wenn die Polizei Datenträger oder Mobiltelefone der eigentlichen Zielpersonen auswertet, auf denen Daten weiterer Personen gespeichert sind. Der Inhalt derartiger Asservate kann jedenfalls gemäß Art. 61a Abs. 1 Satz 1 Halbsatz 2 BayPAG in die Analyse einbezogen werden,

LT-Drs. 19/1557, S. 24.

aaa. Beschwerdeführer*innen zu [XXX]

Die Beschwerdeführer*innen zu [X] stehen beruflich und/oder aufgrund ihrer politischen Aktivitäten mit anderen potenziellen Zielpersonen in Kontakt und laufen daher mit hoher Wahrscheinlichkeit Gefahr, als Kontaktperson von Maßnahmen nach Art. 61a BayPAG betroffen zu sein.

(1) Kontaktpersonen

[…]

(2) Kein ausreichender Schutz für Berufsgeheimnisträger*innen

Die Erfassung von Daten der Beschwerdeführer*innen zu [XXX] wird dabei auch nicht sicher durch die Vorschriften zum Schutz von Berufsgeheimnisträger*innen ausgeschlossen.

Art. 61a BayPAG selbst sieht keine Regelung zum Schutz von Berufsgeheimnisträger*innen vor. Auch aus Art. 49 Abs. 1 BayPAG ergibt sich kein Schutz für Berufsgeheimnisträger*innen, die von Art. 61a BayPAG betroffen sind. Zwar sieht Art. 49 Abs. 1 BayPAG vor, dass die Datenerhebung unzulässig ist und gleichwohl erlangte Erkenntnisse nicht weiterverarbeitet werden dürfen, wenn erkennbar ist oder wird, dass eine Erhebungsmaßnahme in ein durch ein Berufsgeheimnis geschütztes Vertrauensverhältnis eingreift. Die in Art. 49 BayPAG geregelten Schutzvorschriften behandeln alle Berufsgeheimnisträger*innen nach §§ 53 f. StPO gleich,

LT-Drs. 17/20435, S. 72.

Dies gilt jedoch nur für die in Art. 49 Abs. 1 BayPAG abschließend aufgezählten Datenerhebungsmaßnahmen. Als solche ist Art. 61a BayPAG nicht aufgeführt. Eine direkte Anwendung des Art. 49 BayPAG aus dem „2. Unterabschnitt Besondere Befugnisse und Maßnahmen der Datenerhebung“ auf den im „3. Abschnitt Datenspeicherung, -übermittlung und sonstige Datenverarbeitung“ geregelten Art. 61a BayPAG ist aufgrund der systematischen Stellung ausgeschlossen.

Auch ordnet Art. 61a Abs. 1 Satz 3 BayPAG keine entsprechende Anwendung des Art. 49 BayPAG an (anders als für Art. 48 Abs. 1, 3, 4, 53 Abs. 2 Art. 54 Abs. 2 BayPAG). Eine Anwendbarkeit der Norm ergibt sich auch nicht aus der Gesetzesbegründung.

Selbst bei einer Anwendbarkeit von Art. 49 Abs. 1 BayPAG wären von diesem andere Datenerhebungsmaßnahmen, wie die Auswertung sichergestellter Datenträger oder Mobiltelefone oder von Daten aus Zeugenvernehmungen, Identitätsfeststellungen oder anderen offenen Maßnahmen (mit Ausnahme offener Bild- und Tonaufnahmen oder -aufzeichnungen in Wohnungen) nicht erfasst. Auch Daten, die durch den Einsatz von Vertrauenspersonen oder verdeckten Ermittler*innen erhoben werden, sind nicht umfasst,

> *Bär*, in: BeckOK PolR Bayern, 25. Ed. 15.10.2024, PAG Art. 49, Rn. 11;
> LT-Drs. 17/20425, S. 70 f.

Daten aus solchen Maßnahmen können dennoch in Datenbanken und damit in Analysen nach Art. 61a BayPAG geraten.

Zudem greift das Erhebungsverbot erst dann, wenn der*die Beschwerdeführer*in als Berufsgeheimnisträger*in erkannt wird,

> *Bär*, in: BeckOK PolR Bayern, 25. Ed. 15.10.2024, PAG Art. 49, Rn. 16.

Aber sogar für den Fall, dass Beschwerdeführer*innen als Berufsgeheimnisträger*innen identifiziert werden, ist die Datenerhebung nicht vollkommen ausgeschlossen. Art. 49 Abs. 1 Satz 1 BayPAG verbietet die Erhebung nicht generell, sondern setzt einen Eingriff in ein „durch ein Berufsgeheimnis nach den §§ 53, 53a StPO geschütztes Vertrauensverhältnis“ voraus. Damit ist die Erhebung erst dann unzulässig, wenn erkannt wird, dass es sich um geschützte berufliche Kommunikation der Beschwerdeführer*innen handelt.

Zudem lässt Art. 49 Abs. 1 Satz 1 Halbsatz 2 eine Ausnahme von der Schutzvorschrift zu, wenn die Maßnahme gegen Berufsgeheimnisträger*innen selbst gerichtet ist, diese also als Störer*innen Adressat*innen der Maßnahme sind,

Bär, in: BeckOK PolR Bayern, 25. Ed. 15.10.2024, PAG Art. 49, Rn. 17.

Der Schutz von Berufsgeheimnisträger*innen kann aufgrund der weitgehenden Störer*innenbegriffe somit leicht unterlaufen werden. Dies gilt auch im vorliegenden Falle, in dem auch eine Maßnahme gegen die Beschwerdeführer*innen als Zielperson wahrscheinlich ist.

Auch das Verwertungsverbot des Art. 49 Abs. 1 Satz 3 BayPAG lässt die Betroffenheit der Beschwerdeführer*innen nicht entfallen, da es nachgelagert ist und einen Missbrauch nicht sicher ausschließen kann.

Die gleiche Einschränkung gilt im Ausgangspunkt für Art. 49 Abs. 4 Satz 1 BayPAG, wonach auf Auswertungsebene die Weiterverarbeitung verboten ist, wenn sich bei der Auswertung von Daten aus den dort aufgezählten verdeckten Erhebungsmaßnahmen ergibt, dass Inhalte betroffen sind, über die nach §§ 53 f. StPO das Zeugnis verweigert werden könnte.

Auch das Verbot der Weiterverarbeitung von Daten ist auf konkret abschließend genannte Maßnahmen in Art. 49 Abs. 4 Satz 1 BayPAG beschränkt. Zwar geht dieser Katalog über den des Abs. 1 Satz 1 hinaus. Auch erklärt Art. 25 Abs. 3 Satz 2 BayPAG die Norm im Fall einer Sicherstellung von Daten für entsprechend anwendbar. Dennoch gewährt die Norm keinen ausreichenden Schutz, da auch Daten aus anderen insbesondere offenen Erhebungsmaßnahmen im Rahmen von Art. 61a BayPAG zusammengeführt und verarbeitet werden können.

Darüber hinaus setzt das Verarbeitungsverbot voraus, dass sich die Betroffenheit des Berufsgeheimnisses bei der Auswertung „ergeben“ muss. Dass Daten etwa auf einem Mobiltelefon einen Bezug zu den beruflichen Tätigkeiten der Beschwerdeführer*innen aufweisen, ist aber nicht immer ohne weiteres erkennbar. Zu denken ist nur an die Möglichkeit, dass die Zielperson Daten der Beschwerdeführer*innen mit Blick auf journalistische oder anwaltliche Kontakte in ihrem elektronischen Telefonbuch gespeichert hat, ohne dass sich aus dem Eintrag der Zweck des Kontakts ergibt.

Hinzu kommt, dass Art. 49 Abs. 4 Satz 1 BayPAG eine „Auswertung“ der fraglichen Daten voraussetzt. Es ist aber möglich, dass personenbezogene

Daten, die die journalistische bzw. anwaltliche Tätigkeit der Beschwerdeführer*innen betreffen, bei der Polizei vorhanden, aber (noch) nicht ausgewertet worden sind. Das kann etwa dann geschehen, wenn ein Speichermedium bisher zwar ausgelesen, aber noch nicht gesichtet wurde, oder wenn sich die Sichtung auf einen Teil beschränkt hat, der die Beschwerdeführer*innen nicht betrifft. Letzteres dürfte angesichts des Umfangs der auf Mobiltelefonen und anderen Speichermedien vorhandenen Daten mit hoher Wahrscheinlichkeit zu erwarten sein. Die Auswertung der die Beschwerdeführer*innen betreffenden Daten würde dann erstmals im Rahmen der automatisierten Datenanalyse erfolgen. Dass im Anwendungsbereich des Art. 61a BayPAG sichergestellt wird, dass eine Kontrolle nach Art. 49 Abs. 4 Satz 1 BayPAG erfolgt, ist jedoch nicht ersichtlich. Dies dürfte technisch auch kaum umsetzbar sein, weil sich die Frage, ob Daten Inhalte betreffen, über die die Beschwerdeführer*innen zeugnisverweigerungsberechtigt sind, kaum automatisiert beantworten lassen.

Schließlich ist das Fehlerrisiko zu beachten, dass einer nachträglichen Bereinigung des Datenbestandes, wie sie Art. 49 Abs. 4 Satz 1 BayPAG vorsieht, stets immanent ist. Insbesondere bei großen Datenmengen, wie sie beim Auslesen von Speichermedien anfallen, besteht die erhebliche Gefahr, dass Daten, über deren Inhalt die Beschwerdeführer*innen das Zeugnis nach § 53 Nr. 5 StPO verweigern dürfte, übersehen oder falsch zugeordnet werden.

Auch die Löschungsvorgaben des Art. 49 Abs. 5 BayPAG lassen die Betroffenheit nicht entfallen. Anders als für Daten aus dem Kernbereich ist eine absolute Löschungsverpflichtung gerade nicht vorgesehen, sondern nach Art. 49 Abs. 5 Satz 2 BayPAG ist die Verarbeitung der durch Maßnahmen nach Abs. 4 erlangten Daten nur einzuschränken, wenn sie zum Zwecke der Information der Betroffenen oder zur gerichtlichen Überprüfung der Erhebung oder Verwendung noch benötigt werden. Nur falls dies nicht der Fall ist, sind Daten unverzüglich zu löschen (Art. 61a Abs. 5 Satz 3). Darüber hinaus greifen Löschungsverpflichtungen nur im Nachhinein und können einen Missbrauch nicht sicher ausschließen.

Für die Beschränkungen der Erhebung und -verwertung von Daten bzw. aus dem Bereich der Strafverfolgung (§ 160a Abs. 2 Satz 2 bis 4, Abs. 5, § 97 Abs. 5, § 100d Abs. 5 Satz 1 i.V.m. Abs. 2, § 100g Abs. 4 Satz 1, 2, 3, 5 StPO für den Beschwerdeführer zu [X]; § 160a Abs. 1 Satz 1-5, § 97 Abs. 1, 2, § 100d Abs. 5 Satz 1 i.V.m. Abs. 2, § 100g Abs. 4 Satz 1, 2, 3, 5 StPO für die Beschwerdeführerin zu [X]) gelten die vorstehenden Erwägungen entsprechend. Sofern § 160a Abs. 5 StPO andere Vorschriften unberührt lässt, erfasst insbesondere § 100g Abs. 4 StPO nur die Erhebung von nach Abs. 2 in Verbindung mit § 176 Telekommunikationsgesetz (TKG) gespeicherten Daten. Außerdem verweist § 100g Abs. 4 Satz 6 StPO unter anderem auf § 160a Abs. 4 StPO, der eine Ausnahme bei möglicher Verstrickung vorsieht. Hinzu kommt, dass das Beschlagnahmeverbot nach § 97 Abs. 5 Satz 1 StPO nur gilt, wenn sich der betroffene Gegenstand bzw. die betroffenen Daten im Gewahrsam der zeugnisverweigerungsberechtigten Person oder ihrer Redaktion etc. befinden. Datenträger oder Mobilfunkgeräte eines Beschuldigten dürfen demnach auch dann ausgewertet werden, wenn sich darauf Daten des Beschwerdeführers zu [X] befinden, die seiner journalistischen Tätigkeit zuzurechnen sind. Diese Beschränkung gilt auch für das die Beschwerdeführerin zu [X] betreffende Beschlagnahmeverbot gemäß § 97 Abs. 2 Satz 1 StPO.

Allein aufgrund dieser Einschränkung ist ein umfassender Schutz von Daten, über die die Beschwerdeführer*innen zu [X] ihr Zeugnis verweigern könnten, nicht gewährleistet.

bbb. Beschwerdeführer*innen zu [XXX]

Auch die Beschwerdeführer*innen zu […] sind als Drittbetroffene selbst und gegenwärtig betroffen, da ihre Daten mit hoher Wahrscheinlichkeit als Kontaktpersonen in Datenanalysen nach Art. 61a BayPAG einbezogen werden.

[…]

c. Beschwerdeführer*innen mit nachweislich polizeilich gespeicherten Daten

Eine eigene und gegenwärtige Betroffenheit ist jedenfalls dann gegeben, wenn nachweislich Daten in polizeilichen Datentöpfen vorhanden sind, die einer Analyse nach Art. 61a BayPAG zugeführt werden können. In diesem Falle ist es für sie nicht nur wahrscheinlich, sondern sogar sicher, dass sie von Datenanalysen betroffen sind, beziehungsweise sein werden, da insbesondere der bayerische Kriminalitätsaktennachweis und die bayerische Vorgangsverwaltung gemäß Art. 61a Abs. 3 Nr. 1 BayPAG bei Maßnahmen nach allen Tatbestandsvarianten einbezogen werden.

Dabei sind von den Beschwerdeführer*innen die Daten in folgenden Datenbanken gespeichert:

[…]

Die Betroffenheit ist auch dann gegeben, wenn die Sachverhalte der Datenspeicherung bereits einige Jahre zurückreichen, da auch in diesem Falle eine vollumfängliche Löschung der Daten nicht gewährleistet und eine Betroffenheit damit nicht ausgeschlossen ist. Art. 62 Abs. 2 Satz 1 BayPAG sieht nämlich vor, dass eine Löschung von in Dateien gespeicherten personenbezogenen Daten erst erfolgt, wenn festgestellt wird, dass ihre Erhebung oder weitere Verarbeitung unzulässig war oder sie zur Erfüllung einer rechtlichen Verpflichtung gelöscht werden müssen, oder wenn sich bei einer regelmäßigen Überprüfung ergibt, dass ihre Kenntnis für die speichernde Stelle zur Erfüllung der ihr obliegenden Aufgaben nicht mehr erforderlich ist. Dabei ist insbesondere zu berücksichtigen, dass die Polizei die Daten gemäß Art. 54 Abs. 1 BayPAG auch zu anderen Zwecken verarbeiten kann als zu denjenigen, zu denen sie ursprünglich erhoben und gespeichert wurden. Etwas anderes gilt gemäß Art. 54 Abs. 1 Satz 2 BayPAG nur, wenn die Daten aus einem Ermittlungsverfahren oder von einer Person stammen, die einer Straftat verdächtig ist; hier sind die Daten mit Entfall des Tatverdachts zu löschen. Diesbezügliche Nachforschungspflichten bestehen jedoch nicht, sodass eine Löschung nicht gesichert ist. Die Fristen für die regelmäßige Überprüfung betragen gemäß Art. 62 Abs. 2 Nr. 3

Satz 2 i.V.m. Art. 54 Abs. 2 Satz 3 BayPAG bei Erwachsenen in der Regel zehn Jahre. Es ist dabei sehr wahrscheinlich, dass die Daten über die Überprüfungsfristen hinaus gespeichert werden. Überprüfungsfristen stellen kein gesetztes Löschdatum dar, sondern gebieten lediglich eine Prüfung der Voraussetzungen einer weiteren Speicherung. Hinzu kommt, dass die Löschung gemäß Art. 62 Abs. 3 BayPAG unter Umständen auch unterbleiben kann und in diesen Fällen trotz Verarbeitungsbeschränkung auch eine Weiterverarbeitung zur Gefahrenabwehr nach Art. 62 Abs. 3 Satz 1 Nr. 4 i.V.m. Art. 53 Abs. 3 BayPAG erfolgen kann.

Weitere Darlegungen sind den Beschwerdeführer*innen weder möglich noch zumutbar. Insbesondere kann zum Beleg der eigenen gegenwärtigen Betroffenheit nicht verlangt werden, dass sich die Beschwerdeführer*innen selbst einer Straftat oder als mögliche Verursacher*innen einer Gefahr für die öffentliche Sicherheit bezichtigen,

> vgl. BVerfG, Beschluss vom 8. Oktober 2024, 1 BvR 1743/16, 1 BvR 2539/16, Rn. 89; BVerfGE 169, 332 (359 Rn. 61); 169, 130 (155 Rn. 38); 165, 1 (31 f. Rn. 43); 163, 43 (73 Rn. 87); 155, 119 (160 Rn. 75); 133, 277 (312 f. Rn. 86).

3. Unmittelbare Betroffenheit

Die angegriffenen Vorschriften betreffen die Beschwerdeführer*innen auch unmittelbar.

Von einer unmittelbaren Betroffenheit durch ein vollziehungsbedürftiges Gesetz ist, obwohl dieses erst der Umsetzung durch Vollzugsakte bedarf, im Falle heimlicher Überwachungsmaßnahmen auszugehen, wenn Beschwerdeführer*innen den Rechtsweg nicht beschreiten können, weil sie keine Kenntnis von der Maßnahme erlangen oder wenn eine nachträgliche Bekanntgabe zwar vorgesehen ist, von ihr aber aufgrund weitreichender Ausnahmetatbestände auch langfristig abgesehen werden kann,

> BVerfG, Beschluss vom 8. Oktober 2024, 1 BvR 1743/16, 1 BvR 2539/16, Rn. 88; BVerfGE 169, 332 (358 Rn. 60); 169, 130 (154

Rn. 37) 165, 1 (31 Rn. 42); 163, 43 (72 Rn. 85); 162, 1 (53 f. Rn. 99); 155, 119 (159 Rn. 73).

So liegt es hier. Die Datenanalyse und -auswertung nach Art. 61a BayPAG erfolgt heimlich durch die Datenverarbeitungssysteme der Polizei, ohne dass die Betroffenen Kenntnis hiervon erlangen könnten. Eine Benachrichtigung der Zielpersonen und erst recht der Drittbetroffenen ist nicht vorgesehen. Benachrichtigungspflichten sind (nur) in Art. 50 Abs. 1 BayPAG geregelt. Dort werden Maßnahmen nach Art. 61a BayPAG nicht genannt. Der Gesetzgeber geht dabei davon aus, dass Benachrichtigungen bereits im Rahmen der Datenerhebung erfolgen,

LT-Drs. 19/1557, S. 25.

Im Übrigen bestehen weitreichende Zurückstellungsmöglichkeiten und Ausnahmen gemäß Art. 50 Abs. 1 Satz 1, Abs. 3, 4 BayPAG. Gemäß Art. 50 Abs. 4 Satz 4 BayPAG kann die Benachrichtigung auch auf Dauer unterbleiben.

Unmittelbar durch die automatisierten Datenanalysen des Art. 61a BayPAG folgen keine offenen staatlichen Grundrechtseingriffe. Die Ergebnisse der Datenverarbeitungen werden vielmehr als Tatsachengrundlage zur Entscheidungsfindung für weitere auch hochinvasive Gefahrenabwehrmaßnahmen herangezogen. Als Vorfeldmaßnahme wird diese für Betroffene heimliche Überwachungsmaßnahme schon deshalb möglicherweise nie oder sehr spät erkennbar, weil eine Benachrichtigung über die Folgemaßnahme unterbleibt. Selbst wenn jedoch Betroffene erfahren, dass sie Gefahrenabwehrmaßnahmen unterworfen wurden bzw. werden, ist damit nicht sichergestellt, dass der Einsatz der Analysesoftware im Vorfeld dieser Maßnahmen ebenfalls erkennbar wird. Es ist damit davon auszugehen, dass Betroffene von Maßnahmen nach Art. 61a BayPAG in der Regel nie Kenntnis erlangen.

Auch über Auskunftsersuchen können die Beschwerdeführer*innen keine ausreichende Kenntnis von Maßnahmen nach Art. 61a BayPAG erlangen. Ein Auskunftsrecht ergibt sich zwar aus Art. 65 Abs. 1 Satz 1, 2 BayPAG. Die

Auskunft beschränkt sich danach aber auf die Angabe, *ob* die Antragsteller*innen betreffende personenbezogene Daten verarbeitet werden, welche Daten sie betreffen, die Rechtsgrundlage und die Zwecke der Verarbeitung, woher die Daten stammen, wem gegenüber sie offengelegt wurden, für wie lange sie gespeichert werden, welche Rechte die Antragsteller*innen geltend machen können und dass sie beim Landesdatenschutzbeauftragten für den Datenschutz Beschwerde einlegen können. Der Gesetzgeber geht jedoch davon aus, dass durch die Maßnahmen nach Art. 61a BayPAG die Speicherung und Löschung der in den Quellsystemen gespeicherten Daten nicht verändert werde,

> LT-Drs. 19/1557, S. 25.

Daher ist schon unklar, ob Auskünfte nach Art. 65 Abs. 1 Satz 1, 2 BayPAG geeignet sind, den Betroffenen Kenntnis von sie betreffenden Maßnahmen nach Art. 61a BayPAG zu verschaffen.

Hinzu kommt, dass Art. 65 Abs. 2 Satz 1 weitreichende Möglichkeiten vorsieht, von der Auskunft abzusehen oder sie einzuschränken. Die Auskunft hätte mithin nur begrenzte Aussagekraft. Betroffene müssen auch nicht zwangsläufig darüber unterrichtet werden, dass von der Auskunft abgesehen oder die Auskunft eingeschränkt wurde (vgl. Art. 65 Abs. 3 Satz 1 i.V.m. Art. 62 Abs. 5 Satz 4 BayPAG). Darüber hinaus ist es für potenziell Betroffene nicht zumutbar, fortlaufend Auskunftsersuchen zu initiieren, um im Falle einer positiven Auskunft Rechtsschutz zu suchen.

II. Subsidiarität

Gegen formelle Gesetze ist ein Rechtsweg nicht gegeben, weshalb § 90 Abs. 2 Satz 1 BVerfGG der Verfassungsbeschwerde nicht entgegensteht. Auch der Grundsatz der Subsidiarität steht der Zulässigkeit nicht entgegen. Dieser erfordert grundsätzlich, vor Einlegung einer Verfassungsbeschwerde alle zur Verfügung stehenden prozessualen Möglichkeiten zu ergreifen, um eine Korrektur der geltend gemachten Verfassungsverletzung zu erwirken oder eine Grundrechtsverletzung zu verhindern. Das gilt auch,

wenn zweifelhaft ist, ob ein entsprechender Rechtsbehelf statthaft ist und er im konkreten Fall in zulässiger Weise eingelegt werden kann,

> BVerfG, Beschluss vom 25. Juni 2025, 1 BvR 368/22, Rn. 17; BVerfGE 169, 332 (359 f. Rn. 62);169, 130 (155 f. Rn. 40); 165, 1 (32 f. Rn. 45).

Ausnahmen bestehen unter anderem, soweit die Beurteilung einer Norm allein spezifisch verfassungsrechtliche Fragen aufwirft, die das angerufene Gericht zu beantworten hat, ohne dass von einer vorausgegangenen fachgerichtlichen Prüfung verbesserte Entscheidungsgrundlagen zu erwarten wären oder wenn die Anrufung der Fachgerichte offensichtlich sinn- und aussichtslos wäre oder sie sonst nicht zumutbar ist,

> BVerfG, Beschluss vom 25. Juni 2025, 1 BvR 368/22, Rn. 17; BVerfGE 169, 130 (156 f. Rn. 41); 165, 1 (32 f. Rn. 47).

Diese beiden Ausnahmen sind vorliegend gegeben. Statthafte Rechtsbehelfe bestehen für die Beschwerdeführer*innen nicht, da vorbeugender Rechtsschutz gegen die Maßnahmen (**1.**) ebenso wenig möglich ist wie ein Vorgehen gegen Verwaltungsvorschriften (**2.**). Auch nachträglicher Rechtsschutz ist nicht möglich und zumutbar (**3.**). Zudem wirft die Verfassungsbeschwerde auch spezifische verfassungsrechtliche Fragen auf (**4.**).

1. Vorbeugender Rechtsschutz

Eine Anrufung der Fachgerichte im vorbeugenden Rechtsschutz wäre aussichtslos, da eine vorbeugende Unterlassungs- oder Feststellungsklage unzulässig wäre. Diese Klagen würden erfordern, dass die Beschwerdeführer*innen ein konkretes behördliches Verfahren bezeichnen können,

> vgl. zur vorbeugenden Unterlassungsklage BVerwG, Urteil vom 19. März 1974, 1 C 7.73, Rn. 41, juris; Beschluss vom 30. September 1981, 3 B 39.81, Rn. 3; Urteil vom 13. Dezember 2017, 6 A 6/16, Rn. 12, juris; Urteil vom 25. Januar 2023, 6 A 1/22, Rn. 21, juris; Urteil vom 9. November 2023, 10 A 3/23, Rn. 13, juris; *Pietzcker/Marsch*, in: Schoch/Schneider, VwGO, 46. EL August 2024, § 42 Abs. 1 Rn. 163;

vgl. zur Feststellungsklage BVerwG, Urteil vom 17. Januar 1980, 7 C 63.77, Rn. 28, juris; Urteil vom 7. Mai 1987, 3 C 53/85, Rn. 24, juris; Urteil vom 30. Mai 2018, 6 A 3/16, Rn. 53, juris; *Marsch*, in: Schoch/Schneider, VwGO, 46. EL August 2024, § 43 Rn. 17 ff.

Eine Klage „ins Blaue hinein" ist hingegen unzulässig,

vgl. *Pietzcker/Marsch*, in: Schoch/Schneider, VwGO, 46. EL August 2024, § 42 Abs. 1 Rn. 163; BVerwG, Beschluss vom 30. September 1981, 3 B 39.81, Rn. 3.

Kenntnis von einem laufenden Verfahren können die Betroffenen bezüglich der Datenanalyse frühestens erlangen, wenn die bayerische Polizei offene Gefahrenabwehrmaßnahmen durchführt oder das Verfahren in ein offenes strafrechtliches Ermittlungsverfahren überleitet. Dies wird allerdings keineswegs in jedem Fall geschehen, da der Einsatz von Analysesoftware zur Sachverhaltsermittlung oder Entscheidungsfindung im Vorfeld der Maßnahme erfolgt und nicht offengelegt werden muss. Dadurch ist in erheblichem Maße erschwert, dass Beschwerdeführer*innen überhaupt Kenntnis darüber erlangen, ob und wie Maßnahmen nach Art. 61a BayPAG das sicherheitsbehördliche Handeln und mögliche Maßnahmen gegen sie beeinflusst haben. Zudem wird die Datenanalyse zu diesem Zeitpunkt bereits abgeschlossen sein, sodass ein vorbeugender Rechtsschutz zu spät käme.

2. Vorgehen gegen Verwaltungsvorschriften

Verwaltungsvorschriften zur Ausführung von Art. 61a BayPAG sind weder durch das Staatsministerium des Inneren, für Sport und Integration, noch durch das Bayerische Landeskriminalamt veröffentlicht worden, obwohl dies nach verfassungsgerichtlichen Vorgaben notwendig wäre,

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

Auch diesbezügliche Informationsanfragen beim Bayerischen Innenministerium und dem Bayerischen Landeskriminalamt ergaben keine Erkenntnisse, ob diesbezügliche Verwaltungsvorschriften erlassen wurden,

siehe Anfrage vom 20. Mai 2025 an das Bayerische Staatsministerium des Innern, für Sport und Integration, abrufbar unter https://fragdenstaat.de/anfrage/verwaltungsvorschriften-und-interne-vorgaben-zu-art-61a-baypag-bzw-zur-verwendung-der-software-vera/; sowie Anfrage vom 20. Mai 2025 an das Bayerische Landeskriminalamt, abrufbar unter https://fragdenstaat.de/anfrage/verwaltungsvorschriften-und-interne-vorgaben-zu-art-61a-baypag-bzw-zur-verwendung-der-software-vera-1/.

Abgesehen davon, dass ein fachgerichtliches Vorgehen gegen Verwaltungsvorschriften im Wege von § 47 Abs. 1 Nr. 2 VwGO nur in absoluten Ausnahmefällen möglich ist,

Giesberts, in: BeckOK VwGO, 73. Ed. 1.4.2025, VwGO § 47, Rn. 29 m.w.N.; *Panzer/Schoch*, in: Schoch/Schneider, 46. EL August 2024, VwGO § 47 Rn. 25 ff.,

ist es jedenfalls unter Subsidiaritätsgesichtspunkten auch nicht geboten, zunächst fachgerichtlich gegen die Verwaltungsvorschrift zur Ausführung des Art. 61a BayPAG vorzugehen, da es allein um die bereits genannten spezifisch verfassungsrechtlichen Fragestellungen geht. Ein fachgerichtlicher Rechtsschutz in Form einer Normenkontrolle könnte zu dieser Klärung nicht beitragen.

3. Nachträglicher Rechtsschutz

Mangels Benachrichtigungspflicht und hinreichender Auskunftsmöglichkeiten ist auch kein nachträglicher Rechtsschutz gegen die automatisierte Anwendung zur Datenanalyse möglich oder zumutbar (siehe **C.I.3.**).

4. Spezifisch verfassungsrechtliche Fragen

Außerdem wirft die Beurteilung der Norm allein spezifisch verfassungsrechtliche Fragen auf, die das angerufene Gericht zu beantworten hat, ohne dass von einer vorausgegangenen fachgerichtlichen Prüfung verbesserte Entscheidungsgrundlagen zu erwarten wären. Denn die Beschwerdefüh-

rer*innen rügen neben der Verletzung von Grundrechten insbesondere einen Verstoß gegen den Gesetzesvorbehalt sowie den Grundsatz der Normenklarheit und Bestimmtheit. Dabei handelt es sich um rein verfassungsrechtliche Fragestellungen, die das angerufene Gericht zu beantworten hat. Die verfassungsrechtliche Beurteilung hängt nicht von der Klärung von Tatsachen oder der fachrechtlichen Auslegung der einzelnen Tatbestandsmerkmale der angegriffenen Befugnisse ab, sondern maßgeblich von deren hinreichender gesetzlicher Begrenzung, Anleitung und Bestimmtheit.

III. Beschwerdefrist

Die Jahresfrist des § 93 Abs. 3 BVerfGG ist gewahrt. Das BayPAG, zuletzt geändert durch § 1 des Gesetzes zur Änderung des Polizeiaufgabengesetzes und weiterer Rechtsvorschriften vom 23. Juli 2024 (GVBl. S. 247), ist hinsichtlich der anzugreifenden Regelung gemäß § 7 des Änderungsgesetzes am 1. August 2024 in Kraft getreten. Die Jahresfrist endet folglich mit dem 31. Juli 2025.

D. Begründetheit der Verfassungsbeschwerde

Die Verfassungsbeschwerde ist begründet.

Bei Art. 61a Abs. 1 Satz 1BayPAG sowie Art. 61a Abs. 2 Satz 1 Nr. 1 und Nr. 2 BayPAG handelt es sich um schwerwiegende Eingriffe in Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG (Recht auf informationelle Selbstbestimmung und IT-Grundrecht) sowie in Art. 10, Art. 13 GG und Art. 19 Abs. 4 GG (**I.**), die den hier geltenden strengen Anforderungen des Gebots der Verhältnismäßigkeit, wie sie das angerufene Gericht im Datenanalyse-Urteil näher konturiert hat, nicht genügen (**II.**) und die Beschwerdeführer*innen deshalb in ihren Grundrechten verletzen.

I. Schwerwiegender Eingriff in das Grundrecht auf informationelle Selbstbestimmung mangels wirksamer Reduzierung des Eingriffsgewichts

Unter Berücksichtigung des Maßstabs für die Beurteilung der Eingriffsintensität (**1.a.**) und unter Berücksichtigung der Wesentlichkeitstheorie sowie den Grundsätzen der Bestimmtheit und Normenklarheit (**1.b.**) enthält Art. 61a BayPAG keine ausreichenden Einschränkungen (**2.**), die dazu führen, dass die Möglichkeiten der Erkenntnisgewinnung so eingegrenzt sind, dass kein besonders schwerer eigenständiger Eingriff in die informationelle Selbstbestimmung der Betroffenen erfolgen kann. Vielmehr handelt es sich bei allen Tatbestandsvarianten des Art. 61a BayPAG um schwere Eingriffe in Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG sowie in Art. 10 Abs. 1 GG, Art. 13 GG und Art. 19 Abs. 4 GG.

1. Maßstab

Art. 61a BayPAG ist an den im Datenanalyse-Urteil präzisierten Kriterien für die Bestimmung des Eingriffsgewichts (**a.**) sowie an der Wesentlichkeitstheorie sowie den Grundsätzen der Bestimmtheit und Normenklarheit zu messen (**b.**).

a. Kriterien für die Bestimmung des Eingriffsgewichts

Das Eingriffsgewicht ergibt sich erstens aus dem Gewicht der zusammenführenden Weiterverwendung vormals getrennter Daten und zweitens daraus, dass Anwendungen zur automatisierten Datenanalyse ein potenzielles Eigengewicht haben, wenn dadurch neue Erkenntnisse über Personen gewonnen werden können,

vgl. BVerfGE 165, 363 (388 f. Rn. 50),

da somit neue Belastungseffekte entstehen, wodurch sich das Gewicht der individuellen Beeinträchtigung bedeutend erhöhen kann,

BVerfGE 165, 363 (395 ff. Rn. 66 ff.).

Das Eingriffsgewicht hängt von verschiedenen Faktoren ab und kann demgemäß vom Gesetzgeber durch unterschiedliche Vorkehrungen und Kombinationen von Schutzmechanismen beeinflusst werden,

BVerfGE 165, 363 (399 Rn. 75).

Wie schwer das Eigengewicht der automatisierten Anwendung zur Datenanalyse im Einzelfall wiegt, lässt sich anhand bestimmter Kriterien ermitteln, die das angerufene Gericht näher beschrieben hat: Das Eingriffsgewicht wird vor allem durch Art und Umfang der verarbeitbaren Daten sowie die zugelassene Methode der Datenanalyse bestimmt. 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 Eingriff,

BVerfGE 165, 363 (401 Rn. 78).

Je weniger die verwendbaren Daten der Art nach eingeschränkt sind, umso größer ist die zur Verarbeitung gelangende Datenmenge und umso höher ist tendenziell das Eingriffsgewicht,

BVerfGE 165, 363 (401 Rn. 78).

Besonderes Eingriffsgewicht kann der Einsatz komplexer Formen des Datenabgleichs haben,

BVerfGE 165, 363 (404 Rn. 90).

Insgesamt ist die Methode automatisierter Datenanalyse oder -auswertung umso eingriffsintensiver, je breitere und tiefere Erkenntnisse über Personen dadurch erlangt werden können, je höher die Fehler- und Diskriminierungsanfälligkeit ist und je schwerer die softwaregestützten Verknüpfungen nachvollzogen werden können,

BVerfGE 165, 363 (405 Rn. 90).

Durch Begrenzungen der Art und des Umfangs der verarbeitbaren Daten sowie der Methoden kann der Gesetzgeber die Eingriffsintensität mithin steuern.

b. Wesentlichkeit, Bestimmtheit, Normenklarheit

Derartige Beschränkungen sind aber nur dann wirksam, wenn sie unter Wahrung des Gesetzesvorbehalts normenklar und hinreichend bestimmt sind,

vgl. BVerfGE 165, 363 (413 ff. Rn. 110 ff.).

aa. Wesentlichkeitstheorie

Der Gesetzgeber muss die wesentlichen Grundlagen zur Begrenzung von Art und Umfang der Daten und der Verarbeitungsmethoden selbst durch Gesetz vorgeben,

BVerfGE 165, 363 (414 Rn. 112).

Dieses Erfordernis entspringt der Wesentlichkeitstheorie, die das angerufene Gericht in ständiger Rechtsprechung aus grundrechtlichen Gesetzesvorbehalten und dem Rechtsstaatsprinzip (Art. 20 Abs. 3 GG) sowie dem Demokratieprinzip (Art. 20 Abs. 1 und 2 GG) ableitet,

vgl. dazu z.B. BVerfGE 166, 93 (161 Rn. 182); 150, 1 (96 Rn. 191 m.w.N.); grundlegend schon BVerfGE 33, 125 (159 ff., insb. 163); BVerfGE 40, 237 (248 f. Rn. 45); BVerfGE 49, 89 (126 Rn. 76); *Denninger*, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Auflage 2021, B. Rn. 58; zur historischen Entwicklung in der Rechtsprechung

des BVerfG eingehend *Lassahn*, Rechtsprechung und Parlamentsgesetz, 2017, S. 77 ff.

Allerdings kann der Gesetzgeber, soweit eine tiefergehende gesetzliche Normierung nicht praktikabel erscheint, die Verwaltung zur näheren Regelung organisatorischer und technischer Einzelheiten ermächtigen,

BVerfGE 165, 363 (414 Rn. 112).

Die Konkretisierung durch Verwaltungsvorschriften bedarf aber einer gesetzlichen Grundlage. Darin 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,

BVerfGE 165, 363 (414 f. Rn. 113) mit Verweis auf BVerfGE 133, 277 (357 Rn. 183).

Von dieser Delegationsmöglichkeit hat der Gesetzgeber in Art. 61a BayPAG keinen Gebrauch gemacht. Eine Ermächtigung zum Erlass von Rechtsvorordnungen oder Verwaltungsvorschriften findet sich darin nicht.

Daraus folgt, dass Art. 61a BayPAG selbst eine ausreichend hohe Regelungsdichte sicherstellen muss,

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

Macht der Gesetzgeber wie vorliegend von der Delegationsmöglichkeit keinen Gebrauch, muss er die delegationsfähigen Aspekte, also insbesondere technische und organisatorische Einzelheiten selbst regeln.

bb. Bestimmtheit und Normenklarheit

Eng mit der Wesentlichkeitstheorie zusammen hängen der Grundsatz der Bestimmtheit und Normenklarheit.

aaa. Allgemeiner Maßstab im Sicherheitsrecht

Der Gesetzgeber muss die von ihm selbst zu normierenden Maßgaben für die Befugnis zur Durchführung automatisierter Datenanalysen hinreichend bestimmt und normenklar regeln,

BVerfGE 165, 363 (415 Rn. 114).

Anlass, Zweck und Grenzen eines Grundrechtseingriffs müssen in der Ermächtigung bereichsspezifisch, präzise und normenklar festgelegt werden. Die konkreten Anforderungen richten sich nach der Art und der Schwere des Eingriffs,

vgl. BVerfGE 156, 11 (45 f.); 145, 20 (69); 141, 220 (265 Rn. 94); 113, 348 (376); 110, 33 (53 ff.).

Dem Grundsatz der Normenklarheit und Bestimmtheit kommt im Sicherheitsrecht besondere Bedeutung zu. Grundsätzlich sind an die Bestimmtheit und Normenklarheit von Ermächtigungen zur heimlichen Erhebung und Verarbeitung von Daten besonders strenge Anforderungen zu stellen,

BVerfG, Beschluss vom 14. November 2024, 1 BvL 3/22, Rn. 86 m.w.N.; BVerfGE 169, 332 (371 Rn. 95); 169, 130 (186 Rn. 116); 162, 1 (125 f. Rn. 273).

Die hohen Anforderungen tragen dem Umstand Rechnung, dass ein effektiver Schutz gegenüber staatlicher Datenerhebung und -verarbeitung nur auf Grundlage eines ausreichend spezifischen gesetzlichen Normprogramms möglich ist. Heimliche Überwachungsmaßnahmen gelangen den Betroffenen kaum zur Kenntnis und können daher von ihnen auch nur selten angegriffen werden. Der Gehalt der gesetzlichen Regelung kann so nur eingeschränkt im Wechselspiel von Anwendungspraxis und gerichtlicher Kontrolle konkretisiert werden, was der Gesetzgeber durch die hinreichende Bestimmtheit der jeweiligen Normen auffangen muss,

BVerfG, Beschluss vom 14. November 2024, 1 BvL 3/22, Rn. 86 m.w.N.; BVerfGE 169, 332 (371 Rn. 95); 169, 130 (186 Rn. 116); 162, 1 (125 f. Rn. 273); 156, 11 (45 Rn. 87); 113, 348 (376); 110, 33 (53 ff.).

Im Einzelnen unterscheiden sich hierbei die Anforderungen zwar maßgeblich nach dem Gewicht des Eingriffs und sind insoweit mit den jeweiligen materiellen Anforderungen der Verhältnismäßigkeit eng verbunden; bei heimlichen Maßnahmen, die weit in die Privatsphäre hineinreichen können, sind die Bestimmtheitsanforderungen indessen hoch,

> BVerfG, Beschluss vom 14. November 2024, 1 BvL 3/22, Rn. 86 m.w.N.; BVerfGE 169, 332 (371 Rn. 95); 169, 130 (186 Rn. 116); 162, 1 (125 f. Rn. 273).

Bei der Bestimmtheit geht es vornehmlich darum, dass Regierung und Verwaltung im Gesetz steuernde und begrenzende Handlungsmaßstäbe vorfinden und Gerichte eine wirksame Rechtskontrolle vornehmen können. Der Gesetzgeber ist dabei gehalten, seine Regelungen so bestimmt zu fassen, wie dies nach der Eigenart des zu ordnenden Lebenssachverhalts mit Rücksicht auf den Normzweck möglich ist,

> BVerfG, Beschluss vom 14. November 2024, 1 BvL 3/22, Rn. 85; BVerfGE 169, 332 (371 Rn. 93); 169, 130 (186 Rn. 115); 163, 43 (82 Rn. 109); 162, 1 (125 Rn. 272); 156, 11 (45 Rn. 86).

Dem Bestimmtheitserfordernis ist genügt, wenn die Auslegungsprobleme mit herkömmlichen juristischen Methoden bewältigt werden können,

> BVerfG, Beschluss vom 14. November 2024, 1 BvL 3/22, Rn. 85; BVerfGE 169, 332 (371 Rn. 93); 156, 11 (45 Rn. 86).

Verbleibende Unsicherheiten dürfen nicht so weit gehen, dass die Vorhersehbarkeit und Justiziabilität des Handelns der durch die Norm ermächtigten staatlichen Stellen gefährdet sind,

> BVerfGE 169, 332 (371 Rn. 93); 163, 43 (82 Rn. 109); 156, 11 (45 Rn. 86).

Bei der Normenklarheit steht die inhaltliche Verständlichkeit der Regelung im Vordergrund, insbesondere damit Bürger*innen sich auf mögliche belastende Maßnahmen einstellen können,

> BVerfG, Beschluss vom 14. November 2024, 1 BvL 3/22, Rn. 85; BVerfGE 169, 332 (371 Rn. 94); 169, 130 (186 Rn. 115); 163, 43 (83 Rn. 110); 162, 1 (125 Rn. 272); 156, 11 (45 Rn. 86); vgl. *Sommermann*, in: Huber/Voßkuhle, GG, 8. Aufl. 2024, Art. 20 Rn. 289.

Bei heimlichen Maßnahmen muss der Inhalt der einzelnen Norm verständlich und ohne größere Schwierigkeiten durch Auslegung zu konkretisieren

sein. So mag eine Regelung durch Auslegung bestimmbar oder der verfassungskonformen Auslegung zugänglich und damit im verfassungsrechtlichen Sinne bestimmt sein, jedoch geht damit nicht zwingend auch ihre Normenklarheit für die Adressat*innen einher,

> BVerfGE 169, 332 (371 Rn. 94); 163, 43 (83 Rn. 111); 156, 11 (46 R. 88).

bbb. Verweisungen auf andere Normen

Sofern der Gesetzgeber auf andere Normen verweist, gelten besondere Anforderungen an die Normenklarheit (**(1)**). Besondere Anforderungen gelten auch, wenn er auf Normen anderer Gesetzgeber verweist (**(2)**).

(1) Normenklarheit

An einer normenklaren Rechtsgrundlage fehlt es zwar nicht schon deshalb, weil in einer Norm auf eine andere Norm verwiesen wird. Doch müssen Verweisungen begrenzt bleiben, dürfen nicht durch die Inbezugnahme von Normen, die andersartige Spannungslagen bewältigen, ihre Klarheit verlieren und in der Praxis nicht zu übermäßigen Schwierigkeiten bei der Anwendung führen. Unübersichtliche Verweisungskaskaden sind mit den grundrechtlichen Anforderungen daher nicht vereinbar,

> BVerfGE 163, 43 (84 Rn. 112); 162, 1 (125 Rn. 272); 154, 152 (266 Rn. 215).

Die inhaltliche Verständlichkeit der Regelung darf nicht verloren gehen,

> BVerfGE 163, 43 (84 Rn. 112).

Dieses Problem stellt sich vor allem bei Verweisungsketten. Allerdings ist ein Mangel an Normenklarheit auch damit verbunden, dass auf Rechtsgrundlagen verwiesen wird, deren maßgebender Inhalt nur mit Schwierigkeiten erfasst werden kann. Verweist der Gesetzgeber auf andere Regelungen, hat er deshalb einzubeziehen, inwieweit sich diese selbst und für sich genommen bereits im Grenzbereich der Normenklarheit bewegen,

> vgl. BVerfGE 163, 43 (84 Rn. 112).

Das bedeutet aber nicht, dass die Normenklarheit der Verwendung von Verweisungen und Verweisungsketten grundsätzlich entgegensteht, da diese den Normtext entlasten und verhindern können, dass der Gesetzte zu lang und wiederum zu unverständlich werden. Sie können sich also auch als Erleichterung darstellen,

vgl. BVerfGE 163, 43 (85 Rn. 113).

So können die in Bezug genommenen unbestimmte Rechtsbegriffe in einem anderen Regelungskontext gegebenenfalls im Wechselspiel von Anwendungspraxis und gerichtlicher Kontrolle konkretisiert werden, da Sachverhalte von der Norm erfasst sind, die nicht heimlich stattfinden,

vgl. BVerfGE 163, 43 (85 Rn. 114).

In einer wertenden Gesamtbetrachtung ist unter Berücksichtigung möglicher Regelungsalternativen zu entscheiden, ob eine Verweisung mit dem Gebot der Normenklarheit vereinbar ist. Dabei kann insbesondere auch der jeweilige Kreis der Normanwender*innen und -betroffenen von Bedeutung sein,

vgl. BVerfGE 163, 43 (85 Rn. 114) m.w.N.

(2) Verweisungen auf Normen anderer Gesetzgeber

Der Landesgesetzgeber muss nicht alle Einzelheiten des gesetzlichen Tatbestandes selbst festlegen, sondern kann auf andere Regelungen auch eines anderen Normgebers verweisen,

BVerfGE 162, 1 (169 Rn. 384); 153, 310 (343 f. Rn. 79); 143, 38 (55); BVerfGE 141, 143 (176 f.); 29, 198 (210); 26, 338 (366 f.).

Es ist zwischen statischen und dynamischen Verweisungen zu unterscheiden.

Statische Verweisungen auf die Fassung eines Gesetzes, wie sie bei Erlass des Gesetzesbeschlusses galt, sind zulässig,

vgl. BVerfGE 162, 1 (169 Rn. 384) m.w.N.; 153, 310 (343 f. Rn. 79); 143, 38 (57); 41, 143 (176 f.).

Strengere Anforderungen gelten jedoch für dynamische Verweisungen. Diese sind nur im Rahmen von Rechtsstaats- und Demokratieprinzip, mithin insbesondere im Rahmen grundrechtlicher Gesetzesvorbehalte zulässig. Ermächtigen Gesetze zu einem Eingriff in Grundrechte, muss der Gesetzgeber die erforderliche Abwägung des betroffenen Grundrechts mit entgegenstehenden Grundrechten, anderen Verfassungsbelangen und sonstigen schützenswerten Interessen selbst vornehmen. Es muss gewährleistet sein, dass der Gesetzgeber die Abwägungsentscheidung in voller Verantwortung trifft,

BVerfGE 162, 1 (169 f. Rn. 385); 143, 38 (57); 141, 143 (176 f.).

Dies ist bei dynamischen Verweisungen von Landesgesetzen auf bundesgesetzliche Regelungen nicht ohne Weiteres gewährleistet, da der Bundesgesetzgeber nicht verpflichtet ist, in seine Abwägungsentscheidungen Rückwirkung seiner Norm auf landesgesetzgeberische Abwägungsentscheidungen zu berücksichtigen. Aufgrund der Dynamik der Verweisung kann der Landesgesetzgeber nicht abwägen, was er nicht vollständig überblickt. Daher sind dynamische Verweisungen des Landesgesetzgebers auf bundesgesetzliche Normen nur ausnahmsweise dann möglich, wenn die in Bezug genommenen Regelungen ein eng umrissenes Feld betreffen und deren Inhalt im Wesentlichen bereits feststeht,

BVerfGE 162, 1 (169 f. Rn. 385) m.w.N.; 26, 338 (366 f.).

Diese Erwägungen gelten gleichermaßen für Verweise auf europäische Normen, sodass der Maßstab entsprechend übertragbar ist,

vgl. BVerfGE 143, 38 (55 f.); 29, 198 (210).

ccc. Anwendbarkeit datenschutzrechtlicher Vorschriften

Für den Fall, dass sich Maßgaben zur Eingrenzung zulässiger Datenverarbeitung bereits aus Vorschriften des allgemeinen oder des polizeilichen Datenschutzrechts ergeben, führt das angerufene Gericht in seiner Entscheidung zur automatisierten Datenanalyse explizit aus, dass deren Anwendbarkeit auf die Datenanalyse oder -auswertungsbefugnis sowohl für die Behörde als auch für Bürger*innen hinreichend deutlich erkennbar

sein, und es auch hinreichend klar sein muss, was daraus für die praktische Ausgestaltung gerade der Datenanalyse oder -auswertungsbefugnis folgt,

> BVerfGE 165, 363 (415 Rn. 114).

2. Hohes Eingriffsgewicht mangels ausreichender Einschränkungen

Unter Beachtung dieser Maßstäbe ermöglicht die gesetzgeberische Ausgestaltung des Art. 61a BayPAG in allen Tatbestandsvarianten schwere Grundrechtseingriffe,

> so auch zu dem Gesetzentwurf, der, bis auf kleinste Änderungen, der nun geltenden Regelung entspricht *Petri*, Stellungnahme zum Fragenkatalog im Rahmen der Anhörung des Ausschusses für Kommunale Fragen, Innere Sicherheit und Sport zum Gesetzentwurf zur Änderung des Polizeiaufgabengesetzes und weiterer Rechtsvorschriften am 16. Mai 2024 – **Anlage 11**, S. 12, 14; *Zöller*, Schriftliche Stellungnahme zum Gesetzentwurf der Staatsregierung für ein Gesetz zur Änderung des Polizeiaufgabengesetzes und weiterer Rechtsvorschriften vom 9. April 2024 (LT-Drs. 19/1557) – **Anlage 12**, S. 14 ff.

a. Art. 61a Abs. 1 Satz 1 BayPAG

Art. 61a Abs. 1 BayPAG enthält nur sehr geringe Einschränkungen hinsichtlich Art und Umfang der verarbeitbaren Daten (**aa.**). Auch die Methode der Datenverarbeitung ist nicht derart eingeschränkt, dass sie zu einer erheblichen Verminderung des Eingriffsgewichts führt (**bb.**).

aa. Kaum Einschränkungen hinsichtlich Art und Umfang der einbezogenen Daten

Art. 61a Abs. 1 Satz 1 BayPAG ist hinsichtlich Art und Umfang der Daten, die in die Analyse einbezogen werden dürfen, kaum beschränkt.

Dies betrifft Einschränkungen in Bezug auf die Herkunft der Daten, die Menge der Daten oder die Datenarten. Von den einschränkenden Vorkehrungen, die das angerufene Gerich Gericht im Datenanalyse-Urteil benannt hat, hat der Gesetzgeber weitestgehend keinen Gebrauch gemacht.

Im Rahmen der Tatbestandsvariante des Art. 61a Abs. 1 Satz 1 BayPAG ist eine nahezu unbegrenzte Auswertung von Datenbeständen möglich (**aaa.**). Es gibt nur geringe Einschränkungen durch Art. 61a Abs. 4 Satz 1, 2 und Abs. 5 Nr. 3 BayPAG (**bbb.**). Durch die Einbeziehung einer Vielzahl von Daten unbeteiligter Personen steigt deren Risiko, Ziel weiterer Überwachungsmaßnahmen zu werden (**ccc.**). Darüber hinaus sind keine organisatorischen oder technischen Vorkehrungen zur Gewährleistung der Zweckbindung getroffen worden (**ddd.**).

aaa. Nahezu unbegrenzte Auswertung von Datenbeständen

Art. 61a Abs. 1 Satz 1 BayPAG erlaubt es der bayerischen Polizei, nahezu unbegrenzt Daten in die Auswertung einzubeziehen. Art. 61a Abs. 1 Satz 1 BayPAG enthält kaum Einschränkungen hinsichtlich der Datenbestände, Datenarten und Dateiformate (**(1)**), es können Daten aus schwerwiegenden Grundrechtseingriffen einbezogen werden (**(2)**) und Art. 61a Abs. 1 Satz 1 Halbsatz 2 BayPAG führt zu unbeschränkten Erweiterungsmöglichkeiten (**(3)**). Außerdem sind die einbeziehbaren Daten hinsichtlich ihrer Herkunft nicht beschränkt (**(4)**).

(1) Kaum Einschränkung hinsichtlich der Datenbestände, Datenarten und Dateiformate

Die Datenbestände, Datenarten und Dateiformate sind kaum beschränkt.

Gemäß Art. 61a Abs. 1 Satz 1 BayPAG kann die Polizei personenbezogene Daten aus verschiedenen eigenen automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, automatisiert zusammenführen, und darauf bezogen weitere nach diesem Gesetz oder besonderen Rechtsvorschriften erhobene personenbezogene Daten verarbeiten.

Die Datenbestände, die zusammengeführt und analysiert werden sollen, sind nicht abschließend aufgeführt. Die Beschränkung des Art. 61a Abs. 3 BayPAG auf bestimmte polizeiliche Datenbestände gilt ausweislich des Wortlauts nicht für die Tatbestandsvariante des Art. 61a Abs. 1 BayPAG.

Weiterhin ist eine Eingriffsmilderung durch eine Begrenzung zugelassener Datenarten, Dateiformate und der Ausschluss bestimmter biometrischer Daten,

> vgl. zu dieser Einschränkungsmöglichkeit BVerfGE 165, 363 (404 Rn. 87),

für die Tatbestandsalternative nicht gegeben.

Denn die Einschränkungen des Art. 61a Abs. 2 Satz 3 bis Satz 5 BayPAG, die bestimmte Datenarten und zum Teil Daten aus schwerwiegenden Grundrechteingriffen ausschließen, gelten nicht für Art. 61a Abs. 1 Satz 1 BayPAG. Das ergibt sich zum einen aus systematischen Gesichtspunkten, da die Beschränkungen in Absatz 2 verortet sind, der eigene Tatbestandsvarianten in Satz 1 enthält. Darüber hinaus enthalten sowohl Art. 61a Abs. 1 BayPAG in Satz 3 als auch Art. 61a Abs. 2 in Satz 2 eine wortgleiche Vorschrift. Dies wäre überflüssig, bezögen sich die Einschränkungen in Art. 61a Abs. 2 Satz 2 bis 5 BayPAG auch auf Art. 61 Abs. 1 Satz 1 BayPAG. Weiterhin käme es sonst auch zu Widersprüchen. Art. 61a Abs. 1 Satz 2 BayPAG ermöglicht es, für die Tatbestandsvariante des Art. 61a Abs. 1 Satz 1 BayPAG personenbezogene Daten, die durch den Einsatz technischer Mittel in Wohnungen erhoben wurden, unter der einschränkenden Voraussetzung einer dringenden Gefahr zu verarbeiten. Art. 61a Abs. 2 Satz 3 BayPAG schließt das für die beiden Tatbestandsvarianten des Art. 61a Abs. 2 Satz 1 BayPAG hingegen aus.

Unklar ist, warum der Gesetzgeber davon ausgeht, dass der Inhalt forensischer Asservate (Datenträger, Mobiltelefone etc.) bzw. Extrakte hieraus nicht automatisiert einbezogen werden können,

> LT-Drs. 19/1557, S. 24.

Jedenfalls Extrakte davon werden in automatisierten Verfahren, wie Fallbearbeitungssystemen, enthalten sein. Außerdem ist es nicht ausgeschlossen, dass die bayerische Polizei ein entsprechendes automatisiertes Verfahren für forensische Asservate künftig einrichtet. Dafür bedarf es ledig-

lich einer Errichtungsanordnung, die der Zustimmung des Staatsministeriums bedarf, sowie einer Datenschutzfolgenabschätzung (vgl. Art. 64 Abs. 1 und Abs. 2 BayPAG). Bei beiden Voraussetzungen handelt es sich nicht um größere Hürden. Dem Landesbeauftragten für Datenschutz ist lediglich ein Recht zur Stellungnahme eingeräumt (Art. 64 Abs. 2 Satz 6 BayPAG).

Es besteht deshalb grundsätzlich die Möglichkeit, bisher nicht in automatisierten Verfahren gespeicherte Daten, insbesondere unstrukturierte und besonders sensible Daten, wie sie sich beispielsweise auf Smartphones befinden, einzubeziehen.

Auch eine herkunftsbezogene Eingrenzung der Daten derart, dass nur Daten einbezogen werden, die bei der Wahrnehmung bestimmter polizeilicher Aufgaben angefallen sind, wie sie beispielsweise § 2 Satz 1 Halbsatz 1 ATDG beinhaltet (nur Daten aus der Terrorismusbekämpfung),

> vgl. zu dieser Einschränkungsmöglichkeit BVerfGE 165, 363 (403 Rn. 82),

ist nicht vorgesehen.

Insbesondere die Einbeziehung von Daten aus der Vorgangsverwaltung (Art. 54 Abs. 1 BayPAG) in die Datenanalyse stellt sich als besonders intensiv dar. Im bayerischen Vorgangsverwaltungssystem der Polizei (IGVP) waren am 30. August 2022 38.659.637 „Vorgangspersonen“ in 21.849.507 Vorgängen erfasst,

> zu dem Gesetzentwurf, der, bis auf kleinste Änderungen, der nun geltenden Regelung entspricht *Petri*, Stellungnahme zum Fragenkatalog im Rahmen der Anhörung des Ausschusses für Kommunale Fragen, Innere Sicherheit und Sport zum Gesetzentwurf zur Änderung des Polizeiaufgabengesetzes und weiterer Rechtsvorschriften am 16. Mai 2024 – **Anlage 11**, S. 15.

Gleiches gilt für Verkehrsdaten aus Funkzellenabfragen. Diese sind zu Strafverfolgungszwecken nach § 100g Abs. 3 StPO zulässig sowie zur Gefahrenabwehr gemäß Art. 42 Abs. 1 Satz 1 Nr. 1, 43 Abs. 2 Satz 1, Satz 3, 44 Abs. 1 Satz 3 BayPAG,

LG Nürnberg-Fürth, Beschluss v. 31.01.2023 – 18 T 7132/22, BeckRS 2023, 3679.

Daten, die nach § 100g Abs. 3 StPO erhoben wurden, unterliegen zwar einer eingeschränkten Verwendung nach § 479 Abs. 2 Satz 2 StPO. Für Daten aus Funkzellenabfragen zu präventiven Zwecken ist eine Einschränkung nicht ersichtlich.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hat in der mündlichen Verhandlung, die dem Datenanalyse-Urteil vorausging, ausgeführt, dass eine Lieferung bei einer Funkzellenabfrage ungefähr 100.000 Daten enthalte,

BVerfGE 165, 363 (426 Rn. 142).

Damit führt allein die Möglichkeit der Einbeziehung von Daten aus Funkzellenabfragen zu einem potenziell sehr großen Datenumfang.

Die Eingrenzung „soweit erforderlich“ (Art. 61a Abs. 1 Satz 1 BayPAG) stellt keine Beschränkung dar. Zunächst ist schon unklar, ob sich die Einschränkung auch auf die Zusammenführung der eigenen automatisierten Verfahren beschränkt oder ausschließlich auf Halbsatz 2. Aus Gründen der Normenklarheit (siehe oben **D.I.1.b.bb.**) wäre eine entsprechende Klarstellung angezeigt, da die erste Auslegung bedeuten würde, dass schon im ersten Schritt bei der Zusammenführung geprüft werden muss, ob die weiteren Voraussetzungen der Norm vorliegen.

Die Erforderlichkeit bezieht sich jedenfalls auf die „Verarbeitung“ der Daten. Dabei handelt es sich aber lediglich um einen Aspekt der in jedem Fall auf Rechtsfolgenseite durchzuführenden Verhältnismäßigkeitsprüfung. Es liegt daher keine mit § 2 Satz 1 a.E. ATDG vergleichbare Beschränkung vor, wie sie das angerufene Gericht vor Augen hatte,

vgl. zu dieser Einschränkungsmöglichkeit BVerfGE 165, 363 (403 Rn. 83).

(2) Einbeziehung von Daten aus schwerwiegenden Grundrechtseingriffen

Auch liegt keine Eingriffsmilderung durch den Ausschluss der Verarbeitung von Daten, die ursprünglich durch besonders schwere Grundrechtseingriffe erlangt wurden, vor,

> vgl. zu dieser Einschränkungsmöglichkeit BVerfGE 165, 363 (402 Rn. 81).

Vielmehr macht Art. 61a Abs. 1 Satz 2 BayPAG deutlich, dass auch personenbezogene Daten, die durch den Einsatz technischer Mittel in Wohnungen (Art. 41 BayPAG; § 100c StPO) erhoben wurden, einbezogen werden dürfen. Auch Daten aus Online-Durchsuchungen (Art. 45 BayPAG; § 100b StPO) dürfen einbezogen werden. Dabei handelt es sich um Daten, die einen sehr hohen Persönlichkeitsbezug aufweisen.

Auch Verkehrsdaten, die in der Regel aus schwerwiegenden Grundrechtseingriffen stammen und dem Schutz des Art. 10 Abs. 1 GG unterstellt sind,

> *Ogorek*, in: BeckOK GG, 61. Ed. 15.3.2025, Art. 10, Rn. 38,

dürfen einbezogen werden.

Als besonders privat, und damit für die Beurteilung der Eingriffsintensität relevant, stellen sich auch die bei Telekommunikationsüberwachungsmaßnahmen neben den Verkehrsdaten anfallenden Inhaltsdaten dar, die gleichermaßen nicht nur die überwachte Person betreffen, sondern auch Gesprächspartner*innen. Deren Weiterverarbeitung stellt gleichzeitig einen Eingriff in Art. 10 Abs. 1 GG dar.

Neben den Daten aus Telekommunikationsüberwachung (Art. 42 Abs. 1, 3, 4 BayPAG, Art. 43 Abs. 2 BayPAG; § 100a StPO) können auch Daten, die aus dem Einsatz verdeckter Ermittler*innen (Art. 37 BayPAG; § 110a StPO), aus dem Einsatz von Vertrauenspersonen (Art. 38 BayPAG), elektronischer Aufenthaltsüberwachung (Art. 34 Abs. 1 BayPAG), dem Einsatz automatisierter Kennzeichenerkennungssysteme (Art. 39 Abs. 1 BayPAG), Postsicherstellung (Art. 35 Abs. 1 BayPAG), Rasterfahndung (Art. 46 Abs. 1 BayPAG), längerfristiger Observationen (Art. 36 Abs. 1 Nr. 1, Abs. 2

BayPAG; § 163f StPO), oder dem Einsatz technischer Mittel außerhalb von Wohnungen (Art. 36 Abs. 1 Nr. 2, Abs. 2 BayPAG; §§ 100f, 163f StPO) stammen, sowie Nutzungsdaten (Art. 43 Abs. 4 BayPAG; § 100k StPO) einbezogen werden.

Werden Daten mit derart hohem Persönlichkeitsbezug im Rahmen des Art. 61a Abs. 1 Satz 1 BayPAG verarbeitet, um neue Erkenntnisse zu gewinnen, ist die Wahrscheinlichkeit hoch, dass die neu gewonnenen Erkenntnisse besondere private und persönlichkeitsrelevante Informationen enthalten. Dies wirkt eingriffserhöhend,

vgl. BVerfGE 165, 363 (400 Rn. 77).

(3) Unbegrenzte Erweiterungsmöglichkeit durch Art. 61a Abs. 1 Satz 1 Halbsatz 2 BayPAG

Art. 61a Abs. 1 Satz 1 Halbsatz 2 BayPAG sieht – mit der Einschränkung in Art. 61a Abs. 5 Nr. 3 BayPAG – die Möglichkeit vor, die Auswertung unbegrenzt zu erweitern („darauf bezogen weitere nach diesem Gesetz oder besonderen Rechtsvorschriften erhobene personenbezogene Daten verarbeiten"). Lediglich die automatisierte Zusammenführung bezieht sich auf „personenbezogene Daten aus verschiedenen eigenen automatisierten Verfahren", nicht aber die Verarbeitung, die daran anschließt. Diese „Verarbeitung" ermöglicht aber die Auswertung und Analyse von weiteren Daten und ist nicht beschränkt (zur Methode sogleich unter **D.I.2.a.bb.**).

Der zweite Halbsatz birgt das Potenzial einer erheblichen Ausweitung der Daten, die einbezogen werden können.

Zwar kann zur Reduktion der Menge verarbeitbarer Daten auch beitragen, wenn vorgegeben wird, dass Dateien nicht automatisiert einbezogen werden, sondern für jeden Analyse- oder Auswertungsvorgang händisch hinzugezogen werden müssen,

BVerfGE 165, 363 (404 Rn. 88).

Gleichwohl trägt die vorliegende Formulierung nur wenig zur Eingriffsreduzierung bei. Aus dem Wortlaut geht nicht eindeutig hervor, dass nur ein-

zelne für die Ermittlung relevante weitere Daten einbezogen werden können. Die Norm kann vielmehr so ausgelegt werden, dass Normanwender*innen unbegrenzt weitere polizeiexterne Daten in die Analyse einbeziehen können, wenn sie nur irgendeinen beliebigen Bezug zu einer Gefahrenlage sehen. Der Halbsatz verhindert mithin lediglich, dass bei jeder Anwendung schon quasi vorkonfiguriert alle möglichen anderen Datenbanken direkt mit den polizeiinternen Datenbanken zusammengeführt werden. Er ermöglicht aber eine zeitlich auf den einzelnen Anwendungsfalls befristete Anbindung weiterer Systeme.

(4) Keine Herkunftsbeschränkung

Die verarbeitbaren Daten sind auch hinsichtlich ihrer Herkunft nicht beschränkt,

> vgl. zu dieser Einschränkungsmöglichkeit BVerfGE 165, 363 (401 Rn. 79).

Auch „eigene automatisierte Verfahren“ können Daten enthalten, die von anderen Behörden an die bayerische Polizei – gegebenenfalls unter einschränkenden Voraussetzungen – übermittelt wurden, wie beispielsweise von Nachrichtendiensten. Landesfremde Datenbanken werden zwar nicht automatisiert zusammengeführt, können aber manuell importiert werden, ohne, dass eine Beschränkung auf einzelne Daten vorgesehen ist (siehe oben **D.I.2.a.aa.aaa.(3)**). Darunter können sehr wohl auch Daten, die etwa im Informationsverbund gemäß § 29 BKAG gespeichert sind, fallen. Auch aus Dateien der 15 übrigen Landespolizeibehörden, der Zollfahndung, des Bundeskriminalamts und der Bundespolizei, Meldedaten oder aus sonstigen Quellen stammende Daten können somit dem Grunde nach in den Analyseverbund einbezogen werden,

> zu dem Gesetzentwurf, der, bis auf kleinste Änderungen, der nun geltenden Regelung entspricht *Petri*, Stellungnahme zum Fragenkatalog im Rahmen der Anhörung des Ausschusses für Kommunale Fragen, Innere Sicherheit und Sport zum Gesetzentwurf zur Änderung des Polizeiaufgabengesetzes und weiterer Rechtsvorschriften am 16. Mai 2024 – **Anlage 11**, S. 17.

bbb. Geringe Einschränkungen durch Art. 61a Abs. 4 Satz 1, 2 und Abs. 5 Nr. 3 BayPAG

Die einzigen für Art und Umfang der Daten relevanten Einschränkungen der Ermächtigungsgrundlage nach Art. 61a Abs. 1 BayPAG finden sich in Art. 61a Abs. 4 Satz 1, 2 und Abs. 5 Nr. 3 BayPAG. Diese mindern das Eingriffsgewicht aber nur unerheblich.

Gemäß Art. 61a Abs. 5 Nr. 3 BayPAG ist der unmittelbare automatisierte Abgleich von personenbezogenen Daten aus der Allgemeinheit offenstehenden Netzwerken nicht zulässig. Darunter sollen ausweislich der Gesetzesbegründung beispielsweise das Internet und die sozialen Medien fallen. Ausgeschlossen ist damit aber lediglich die direkte automatisierte Einbindung und automatisierte Auswertung dieser Quellen,

LT-Drs. 19/1557, S. 24.

Die Daten dürfen also durchaus, nur eben nicht automatisiert, aber gegebenenfalls in großer Menge einbezogen werden.

Weiterhin handelt es sich bei Art. 61a Abs. 4 Satz 1 BayPAG um eine eingriffsreduzierende Beschränkung.

Art. 61a Abs. 4 Satz 1 BayPAG sieht eine Zugriffsbeschränkung auf besonders ausgewähltes und geschultes Personal vor: Gemäß Art. 61a Abs. 4 Satz 2 BayPAG sind die Zugriffsmöglichkeiten des eingesetzten Personals auf die gemäß den Absätzen 1 und 2 zur Verfügung stehenden personenbezogenen Daten durch technische und organisatorische Maßnahmen auf das erforderliche Maß zu beschränken. Die technisch und organisatorisch gesicherte Beschränkung des Zugriffs lediglich einer begrenzten Zahl von Mitarbeitenden und eine besondere Qualifizierung dieser Personen kann praktisch die Menge der durch Datenanalyse oder -auswertung verarbeitbaren personenbezogenen Daten begrenzen,

BVerfGE 165, 363 (404 Rn. 89).

Soweit die Zugriffsmöglichkeiten auf das „erforderliche Maß“ zu beschränken sind, bestehen aber verfassungsrechtliche Zweifel hinsichtlich der Normenklarheit und des Wesentlichkeitsgrundsatzes (siehe oben zum

Maßstab **D.I.1.b.**). Für Bürger*innen ist nicht ansatzweise nachvollziehbar, welche Daten für welche geschulten Beamt*innen erforderlich sind. Dafür gibt das Gesetz keine Kriterien vor. Zwar erscheint es möglich, dafür Regelungen in einer Verwaltungsvorschrift zu treffen. Davon hat der Gesetzgeber aber keinen Gebrauch gemacht. Da die Anforderungen an die Regelungsdichte deshalb besonders hoch sind (siehe oben **D.I.1.b.aa.**), hätte der Gesetzgeber hier spezifischere Angaben im Normtext selbst machen müssen, um eine beschränkende Wirkung wirksam zu erzielen.

Die Datenmenge wird auch durch Regelungen über Aufbewahrungsfristen und Löschungspflichten bestimmt,

> BVerfGE 165, 363 (403 Rn. 85).

Laut der Gesetzesbegründung zieht ein Zusammenführen von Daten keine Verlängerung der Speicherfristen in den Quellsystemen im Sinn des Art. 54 Abs. 2 Satz 6 PAG nach sich,

> LT-Drs. 19/1557, S. 25.

Diese Einschränkung findet sich allerdings nicht im Normtext wieder. Eine Klarstellung wäre angezeigt, da das Zusammenführen auch eine Speicherung beinhalten kann, und es damit nicht hinreichend deutlich ausgeschlossen ist, dass es zu einer Verlängerung der Frist kommt.

Für Daten, die nicht in eigenen automatisierten Verfahren gespeichert sind, sondern manuell hinzugezogen wurden, legt Art. 61a BayPAG darüber hinaus nicht fest, ob diese nach Abschluss der Ermittlungen in dem System verbleiben und damit Gegenstand weiterer Analysen werden können oder gelöscht werden müssen. Darin liegt die Möglichkeit begründet, den zusammengeführten Datenbestand auch über den Einzelfall hinaus konstant zu erweitern.

ccc. Einbeziehung einer Vielzahl von Daten Unbeteiligter

Eingriffsmildernd wirkt zudem, wenn lediglich Daten Verwendung finden, die sich auf Personen beziehen, bezüglich derer die Polizei tatsächliche An-

haltspunkte besitzt, dass diese selbst in (hinreichend gewichtige) Straftaten verfangen sind oder dass sie Kontaktperson zu einer solchen Person sind,

> BVerfGE 165, 363 (403 Rn. 83).

Eine solche Begrenzung ist für Art. 61a Abs. 1 Satz 1 nicht vorgesehen.

Als besonders bedenklich stellt sich die Einbeziehung von Vorgangsdaten und von Verkehrsdaten, speziell aus Funkzellenabfragen, dar (siehe dazu oben **D.I.2.a.aa.aaa.(1)**). Diese Daten betreffen typischerweise in hoher Zahl vor allem unbeteiligte Personen, die noch nie polizeilich in Erscheinung getreten sind. Außerdem können auch Asservate, beispielsweise Datenträger wie USB-Sticks, Festplatten, Smartphones und Laptops, große Mengen personenbezogener Daten Unbeteiligter enthalten. Durch die Einbeziehung dieser Daten besteht für Unbeteiligte ein hohes Risiko Adressat*innen weiterer Maßnahmen zu werden. Dies wirkt sich eingriffserhöhend aus.

Die Vorgangsverwaltung dient der formalen Begleitung eines Vorgangs, also dazu, die bei einer Dienststelle anfallenden Informationen, wie etwa Anfragen oder Anzeigen in geordneter Form aufzubewahren und ein Wiederauffinden zu ermöglichen,

> *Müller/*Schwabenbauer, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, G. Informationsverarbeitung im Polizei- und Strafverfahrensrecht, Rn. 832 m.w.N.

Ihr kommt somit lediglich eine Hilfsfunktion zu,

> *Müller/*Schwabenbauer, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, G. Informationsverarbeitung im Polizei- und Strafverfahrensrecht, Rn. 833.

Aufgenommen werden beispielweise Daten aus Ermittlungsvorgängen, wie Anzeigen, Ermittlungsberichte, Vermerke oder auch bei Verkehrsunfällen aufgenommene Daten. Darüber hinaus enthalten sie aber auch Daten zu Anzeigeerstatter*innen, Zeug*innen, Hinweisgeber*innen, Unfallbeteiligten und anderen Personen, die nicht Verdächtige oder Beschuldigte im

Sinne des Strafprozessrechts oder Verantwortliche im Sinne des Polizeirechts sind,

> *Arzt*, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, G. Informationsverarbeitung im Polizei- und Strafverfahrensrecht, Rn. 1184 m.w.N.

Es handelt sich also um Daten, für die eine abschließende Sachverhaltsbeurteilung noch aussteht. Aus diesem Grund werden Vorgangsdaten in der Regel nicht in polizeiliche Ermittlungen einbezogen und auch bei Auskunftsersuchen gesondert ausgewiesen.

Die Mehrzahl der im bayerischen Vorgangsbearbeitungssystem (IGVP) am 30. August 2022 gespeicherten Personen war weder einer Straftat oder Ordnungswidrigkeit verdächtig oder von polizeilichen Eingriffsmaßnahmen betroffen (sogenannte „B-Personen“), sondern Zeugen, Geschädigte, Auskunftspersonen etc. (sogenannte „Z-Personen“),

> zu dem Gesetzentwurf, der, bis auf kleinste Änderungen, der nun geltenden Regelung entspricht *Petri*, Stellungnahme zum Fragenkatalog im Rahmen der Anhörung des Ausschusses für Kommunale Fragen, Innere Sicherheit und Sport zum Gesetzentwurf zur Änderung des Polizeiaufgabengesetzes und weiterer Rechtsvorschriften am 16. Mai 2024 – **Anlage 11**, S. 15.

Hinzu kommt, dass die Polizei theoretisch ohne Weiteres die Möglichkeit hat, etwa durch eine extensivere Dokumentation ihres Handelns das Volumen der in IGVP gespeicherten Daten eigenständig und kaum normativ begrenzt zu erhöhen,

> zu dem Gesetzentwurf, der, bis auf kleinste Änderungen, der nun geltenden Regelung entspricht *Petri*, Stellungnahme zum Fragenkatalog im Rahmen der Anhörung des Ausschusses für Kommunale Fragen, Innere Sicherheit und Sport zum Gesetzentwurf zur Änderung des Polizeiaufgabengesetzes und weiterer Rechtsvorschriften am 16. Mai 2024 – **Anlage 11**, S. 16.

Ferner enthalten auch Verkehrsdaten, insbesondere solche, die aus Funkzellenabfragen oder aus Telekommunikationsüberwachungsmaßnahmen

stammen, aufgrund ihrer Streubreite typischerweise eine Vielzahl von Daten Unbeteiligter.

Aber auch sonstige Datenbestände sind nicht frei von Daten von Personen, die bisher keinen Bezug zu polizeilichen Ermittlungs- oder Gefahrenabwehrmaßnahmen hatten (z.B. Falldaten, Asservate, Telekommunikationsdaten).

Mangels entsprechender Beschränkungen erhöht Art. 61a Abs. 1 Satz 1 BayPAG mithin das Risiko für objektiv Unbeteiligte, Ziel weiterer polizeilicher Aufklärungsmaßnahmen zu werden. Dies spricht für ein hohes Eingriffsgewicht,

BVerfGE 165, 363 (400 Rn. 77).

Eine Kennzeichnung von Daten Unbeteiligter sieht das Gesetz nicht vor.

ddd. Keine organisatorischen oder technischen Vorkehrungen zur Gewährleistung der Zweckbindung

Der Umfang der verarbeitbaren Daten ist auch nicht durch organisatorische oder technische Vorkehrungen zur Sicherstellung der Zweckbindung gewährleistet.

Insbesondere Regelungen zur Sicherung der Zweckbindung tragen zugleich zu einer Begrenzung des Datenumfangs bei. Wenn durch organisatorische oder technische Vorkehrungen gesichert wird, dass Daten nur ihrer rechtlichen Verwendbarkeit gemäß weiterverarbeitet werden und wenn die rechtliche Verwendbarkeit hinreichend eng gefasst ist, kann dies den Umfang der verarbeitbaren Daten erheblich reduzieren. Technisch-organisatorische Sicherungen, die die Einhaltung der Zweckbindung sicherstellen, können etwa in der technischen Trennung von Datenbeständen nach unterschiedlichen Verarbeitungszwecken oder in einer zweckabhängigen Verteilung von Zugriffsrechten auf Datenbestände bestehen,

BVerfGE 165, 363 (402 Rn. 80) m.w.N.

Zwar stellt Art. 61a Abs. 1 Satz 3 und Abs. 2 Satz 2 BayPAG klar, dass die Vorschriften des Art. 48 Abs. 1, 3 und 4 BayPAG, des Art. 53 Abs. 2 BayPAG

sowie des Art. 54 Abs. 2 Satz 1 BayPAG unberührt bleiben. Außerdem ist die Verarbeitung von personenbezogenen Daten, die durch den Einsatz technischer Mittel in Wohnungen erhoben wurden, an das Vorliegen einer dringenden Gefahr geknüpft (Art. 61a Abs. 1 Satz 2 BayPAG). Die Anwendbarkeit weiterer speziellerer Regelungen über die Weiterverarbeitung von Daten, wie beispielsweise § 479 Abs. 2 StPO, ist hingegen nicht geregelt. Entgegen der verfassungsrechtlichen Anforderungen ist die Anwendbarkeit weder für die Behörde noch für Bürger*innen hinreichend deutlich erkennbar, und es ist auch nicht hinreichend klar, was daraus für die praktische Ausgestaltung gerade der Datenanalyse oder -auswertungsbefugnis folgt (siehe oben **D.I.1.b.bb.ccc.**).

Weiterhin ist die Wirkung dieser Vorschriften ohnehin nicht durch Maßgaben zur technischen und organisatorischen Umsetzung praktisch hinreichend gesichert, um das Eingriffsgewicht der Datenanalyse oder -auswertung hierdurch erheblich zu mindern.

Bei der automatisierten Analyse oder Auswertung großer Datenbestände, die zudem teils automatisiert einbezogen werden, können Regelungen über die Zweckbindung ihre begrenzende Wirkung auch aus praktischen Gründen nicht ohne Weiteres entfalten, weil die Menge der Daten und deren teils automatisierte Einbindung eine Zweckidentifizierung und -prüfung für jedes einzelne Datum erschweren,

> BVerfGE 165, 363 (424 Rn. 138).

Deshalb fordert das angerufene Gericht für die praktische Umsetzung der Grundsätze der Zweckbindung und Zweckänderung insbesondere eine entsprechende Kennzeichnung der Daten,

> BVerfGE 165, 363 (394 f. Rn. 65).

Die Vorgaben des angerufenen Gerichts erfordern für die technische Umsetzung eine umfassende Mikrokategorisierung,

> vgl. *Hartmann/Cipierre/Beeck*, RDV 2023, 147 (150).

Weder schreibt Art. 61a BayPAG eine ausreichende Unterscheidung nach Herkunft und Erhebungszwecken vor, noch wird eine entsprechende Kennzeichnungspflicht im Gesetzestext explizit festgeschrieben.

Sofern sich Kennzeichnungspflichten aus Art. 48 Abs. 5 BayPAG ergeben, ist schon nicht klar, ob die Norm bei der Datenanalyse nach Art. 61a BayPAG überhaupt eine Rolle spielt.

Gemäß Art. 48 Abs. 5 Satz 1 BayPAG sind personenbezogene Daten, die durch die in den Abs. 1 und 4 bezeichneten Maßnahmen erhoben wurden, besonders zu kennzeichnen. Gemäß Satz 2 ist bei Daten, die unter Inanspruchnahme von Diensteanbietern nach Art. 43 Abs. 2 BayPAG erlangt wurden, dabei auch zwischen Daten nach § 3 Nr. 70 TKG und § 9 Abs. 1 TDDDG und Daten nach § 176 TKG zu unterscheiden. Die Kennzeichnungspflicht betrifft damit Daten aus schwerwiegenden Grundrechtseingriffen.

E contrario Art. 61a Abs. 1 Satz 3 BayPAG und Art. 61a Abs. 2 Satz 2 BayPAG müssen Normanwender*innen und Betroffene mangels Bezugnahme davon ausgehen, dass die Kennzeichnungspflicht im Gegensatz zu den Zweckbindungsgrundsätzen keine Anwendung finden soll. Um der verfassungsrechtlichen Anforderung der Normenklarheit mit Blick auf die Anwendbarkeit datenschutzrechtlicher Vorschriften zu genügen (siehe oben **D.I.1.b.bb.ccc.**), hätte der Gesetzgeber explizit auf Art. 48 Abs. 5 BayPAG verweisen müssen.

Die Norm ist außerdem gemäß Art. 101 BayPAG i.V.m. Art. 102 Abs. 2 BayPAG bis zum 25. Mai 2028 ausgesetzt, sodass sogar, wenn Art. 48 Abs. 5 BayPAG auf Art. 61a PAG anwendbar wäre, die Zweckbindung jedenfalls bis zu diesem Zeitpunkt nicht gesichert wäre. Darüber hinaus ist aus denselben Gründen auch unklar, ob und inwiefern die in Art. 48 Abs. 7 BayPAG vorgesehene Sicherung gegen unbefugte Kenntnisnahme, Veränderung und Löschung bei Verwendung der Daten zur Analyse fortbestehen soll.

Zudem ist in der Norm durch das uneingeschränkt vorgesehene „Zusammenführen“ von Daten (dazu sogleich **D.I.2.a.bb.aaa.(1)**) nicht klar ausgeschlossen, dass sämtliche einbezogene Daten nicht nur anlassbezogen, sondern dauerhaft und unabhängig von einem konkreten Anlass abrufbar

sind. Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit sieht in der dauerhaften Anlegung einer Datenbank zur Datenanalyse einen über die Zusammenführung hinausgehenden, äußerst schwerwiegenden Grundrechtseingriff,

> vgl. zu einer Befugnis zu den Entwürfen ähnliche Befugnisse zur Datenanalyse auf Bundesebene *Bundesbeauftragte für den Datenschutz und die Informationsfreiheit,* Stellungnahme zum Entwurf eines Gesetzes zur Verbesserung der Terrorismusbekämpfung, BT-Drs. 20/12806, Ausschuss-Drs. 20(4)483, S. 7 ff. zum Entwurf eines § 16a BKAG im Sicherheitspaket der Ampelregierung, sie spricht insoweit von einer „Super-Datenbank".

Auch aus diesem Grunde ist die Zweckbindung nicht gesichert.

bb. Unzureichende Einschränkung der Methoden der Datenanalyse

Auch die zugelassene Methode beeinflusst die Eingriffsintensität,

> BVerfGE 165, 363 (404 ff. Rn. 90 ff.).

Da die Methode der automatisierten Datenanalysen in Art. 61a BayPAG nicht wirksam beschränkt ist, sondern vielmehr auch komplexe Analysen zulässt, den Einsatz von Künstlicher Intelligenz (KI) nicht hinreichend klar und vollständig ausschließt und keine Vorkehrungen zur Verhinderung der Realisierung von Diskriminierungsrisken geregelt sind, handelt es sich auch unter diesem Gesichtspunkt um einen schwerwiegenden Eingriff.

Der Gesetzgeber muss grundlegende Maßgaben zur Begrenzung des Automatisierungsgrades selbst treffen. Es reicht nicht aus, dass die Polizeibehörden die Datenanalyse oder -auswertung faktisch so gestalten, dass sie nicht über einen einfachen Datenabgleich in automatisierter Form hinausgeht, insbesondere nicht automatisiert wiederholte Abgleichschritte zur Verknüpfung der Abgleichergebnisse mit weiteren Datenbeständen erfolgen. Eine Beschränkung der Abgleichmöglichkeiten müsste vielmehr im Gesetz selbst angelegt sein,

> BVerfGE 165, 363 (417 ff. Rn. 121).

Eine solche Beschränkung findet sich in Art. 61a BayPAG aber gerade nicht. Die Norm sieht weder ausreichende Beschränkungen der Analysemethode (**aaa.**) noch Vorkehrungen zur Vermeidung von Diskriminierungen (**bbb.**) vor.

aaa. Keine zureichende Beschränkung der zugelassenen Methode

Nach Art. 61a Abs. 1 Satz 1 kann die Polizei die zuvor dargestellten personenbezogene Daten „automatisiert zusammenzuführen und darauf bezogen weitere nach diesem Gesetz oder besonderen Rechtsvorschriften erhobene personenbezogene Daten verarbeiten", dies erfolgt ausdrücklich „zur Gewinnung neuer Erkenntnisse".

Die Norm ermöglicht komplexe Datenanalysen (**(1)**) und sieht keine ausreichenden Einschränkungen der Methode in Art. 61a Abs. 4 Satz 3 sowie in Abs. 5 Nr. 1 und Nr. 2 BayPAG vor (**(2)**). Weitere Beschränkungen sind im Gesetzeswortlaut nicht angelegt (**(3)**).

(1) Ermöglichung einer umfassenden, methodenoffenen Datenanalyse

Art. 61a BayPAG erlaubt weit mehr als nur die Verbindung zuvor getrennter polizeilicher Datensätze. Art. 61a Abs. 1 Satz 1 BayPAG ist methodenoffen formuliert und ermöglicht umfassende komplexe automatisierte Datenanalysen der zusammengeführten und gegebenenfalls weiterer im Einzelfall hinzugefügter Daten.

Nach Art. 61a Abs. 1 Satz 1 BayPAG kann die Polizei „zur Gewinnung neuer Erkenntnisse personenbezogene Daten aus verschiedenen eigenen automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, automatisiert zusammenführen und darauf bezogen weitere nach diesem Gesetz oder besonderen Rechtsvorschriften erhobene personenbezogene Daten verarbeiten".

Zwar spricht die Befugnis nicht explizit von Analyse oder Auswertung. Allerdings sprechen Wortlaut, Systematik, Entstehungsgeschichte und Sinn und Zweck des Art. 61a BayPAG für dieses Verständnis.

Aus dem Wortlaut ergibt sich, dass Maßnahmen nach Art. 61a Abs. 1 Satz 1 BayPAG gerade „zur Gewinnung neuer Erkenntnisse“ erfolgen. Die technischen Mittel sollen also Erkenntnisse bringen, die so noch nicht vorlagen, indem sie bislang nicht bekannte Beziehungen in den Daten offenlegen und Muster erkennen.

Die Befugnis enthält zwei Verarbeitungsvorgänge, „zusammenführen“ in Halbsatz 1 und „verarbeiten“ in Halbsatz 2, ohne dass die Vorgänge gesetzlich näher definiert werden.

Weder das BayPAG noch das BayDSG sehen eine Definition der Verarbeitung vor. Für den Begriff der Verarbeitung in Halbsatz 2 kann aber der Begriff aus Art. 3 Nr. 2 der JI-Richtlinie bzw. dem gleichlautenden Art. 4 Nr. 2 Datenschutzgrundverordnung (DSGVO) herangezogen werden. Verarbeitung umfasst damit

> „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung“
>
> Art. 3 Nr. 2 JI-Richtlinie.

Unter diese Definition fällt aber auch das nicht näher präzisierte „automatisierte Zusammenführen“, das aus mehreren verschiedenen Verarbeitungsschritten bestehen kann.

Sowohl die automatisierte Zusammenführung in Halbsatz 1 als auch die Verarbeitung in Halbsatz 2 stellen daher Verarbeitungen im Sinne von Art. 3 Nr. 2 der JI-Richtlinie bzw. dem gleichlautenden Art. 4 Nr. 2 DSGVO dar.

Eine Einschränkung der Verarbeitungsmethode ist im Wortlaut für beide Verarbeitungsvorgänge nicht angelegt. Daher werden grundsätzlich methodenoffene und automatisierte Vorgänge und Vorgangsreihen ermöglicht.

Eine Ermächtigung zur Datenanalyse ergibt sich nach dem gesetzgeberischen Verständnis bereits aus „automatisiert zusammenführen".

Unter „zusammenführen" ist grundsätzlich zu verstehen, dass Daten aus zunächst getrennten Datentöpfen miteinander verbunden werden, dass also bestehende Trennungen zwischen Datensätzen aufgehoben werden. Schon die Zusammenführung stellt dabei eine bestimmte Form der Verarbeitung und einen eigenständigen Eingriff in Grundrechte, insbesondere die informationelle Selbstbestimmung dar. Das Zusammenführen erfolgt dabei „automatisiert", also mit Hilfe von technischen Mitteln in Form von Software.

Zwar geht der Gesetzgeber einerseits davon aus, dass Art. 61a Abs. 1 BayPAG aufgrund der automatisierten, datenbank- und formatübergreifenden vollständigen Zusammenführung die teilweise technisch bedingte oder durch den Zweck der jeweiligen Errichtungsanordnung gebotene Trennung der unterschiedlichen Datenbanken überwindet, ohne die Datenanalyse an dieser Stelle zu erwähnen,

> „Abs. 1 überwindet aufgrund der automatisierten, datenbank- und formatübergreifenden vollständigen Zusammenführung die teilweise technisch bedingte oder durch den Zweck der jeweiligen Errichtungsanordnung gebotene Trennung der unterschiedlichen Datenbanken […]"
>
> LT-Drs. 19/1557, S. 24 a.E.

Allerdings impliziert „automatisiertes Zusammenführen" bereits eine automatisierte und softwarebasierte Kombination und daran anschließend automatisierte Kategorisierung, Anpassung und Veränderungen der Daten dergestalt, dass eine gemeinsame Nutzung der kombinierten Daten überhaupt möglich ist. Beispielsweise müssen so unterschiedliche Datenformate angepasst und verarbeitbar gemacht werden.

Gleichzeitig erfolgt die Zusammenführung nach Gesetzeswortlaut „zur Gewinnung neuer Erkenntnisse“. Die Gesetzesbegründung spricht in Bezug auf die Zusammenführung in Halbsatz 1 von „diese neuen Erkenntnisse“ und „Ergebnis der Recherche“. Darüber hinaus geht der Gesetzgeber davon aus, durch das Zusammenführen erfolge eine „automatisierte[…] Zusammenführung des Abgleichergebnisses“ und eine „Zusammenführung der Trefferfälle“,

> LT-Drs. 19/1557, S. 24.

Der Gesetzgeber nimmt daher erkennbar an, dass die „Zusammenführung“ zu „Abgleichergebnissen“ und zu „Trefferfällen“ führt. Die Gesetzesbegründung insinuiert insoweit eine sehr weite Auslegung des Begriffs des Zusammenführens, die gerade auch eine Verarbeitung von Daten umfasst, durch die Auswertungs- und Analyseergebnisse erzielt werden. „Automatisiert zusammenführen“ ermächtigt nach der vom Gesetzgeber vertretenen Auslegung auch, die Daten automatisiert zueinander in Bezug zu setzen, Verbindungen aufzudecken oder herzustellen und dabei auch eine inhaltliche Auswahl unter den vorhandenen Daten zu treffen. Damit umfasst die Zusammenführung eine automatisierte Datenauswertung und -analyse.

Jedenfalls ergibt sich eine Ermächtigung zur Datenanalyse aus der Ermächtigung zur „darauf bezogenen Verarbeitung“ in Art. 61a Abs. 1 Satz 1 Halbsatz 2 BayPAG.

„Verarbeiten“ von Daten ist wie dargestellt ein weiter Begriff, für den die Definitionen der Datenverarbeitung aus Art. 3 Nr. 2 der JI-Richtlinie bzw. dem gleichlautenden Art. 4 Nr. 2 DSGVO herangezogen werden kann. Verarbeitung umfasst daher

> „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch

> Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung“
>
> Art. 3 Nr. 2 JI-Richtlinie.

Der Begriff gibt keine bestimmte Methode der Datenauswertung vor. Die Datenverarbeitung ist gerade nicht auf einen bloßen Datenabgleich beschränkt, sondern ist methodenoffen möglich. Der Begriff ermöglicht damit eine umfassende automatisierte Datenverarbeitung und -analyse mit komplexen Algorithmen.

Insbesondere ist dabei nicht von Belang, dass die Verarbeitung nicht explizit als automatisiert geregelt ist, wie es für die Zusammenführung in Halbsatz 1 vorgesehen ist. Der Begriff der Verarbeitung nach Art. 3 Nr. 2 JI-Richtlinie sieht als Verarbeitung sowohl Vorgänge „mit und ohne Hilfe automatisierter Verfahren“ an.

Art. 61a Abs. 1 Satz 1 Halbsatz 2 BayPAG ist daher Rechtsgrundlage für jede weitere auch automatisierte Verarbeitung der nach Art. 61a Abs. 1 Satz 1 Halbsatz 1 BayPAG zusammengeführten Daten.

Dem steht auch die in der Gesetzesbegründung angenommene Zweistufigkeit des Art. 61a Abs. 1 Satz 1 BayPAG nicht entgegen. Der Gesetzgeber führt aus, dass Halbsatz 2 die Möglichkeit bereitstelle, dem „Ergebnis nach der erfolgten automatisierten Zusammenführung des Abgleichergebnisses und dessen anschließender Bewertung, Informationen und Erkenntnisse anwenderbezogen für die weitere Ermittlung hinzuzufügen“,

> LT-Drs. 19/1557, S. 24.

Diese strenge Zweistufigkeit findet keinen Niederschlag im Gesetzeswortlaut selbst, denn Art. 61a Abs. 1 Satz 1 Halbsatz 2 BayPAG gestattet die völlig methodenoffene Verarbeitung „darauf bezogen“ und damit auch hinsichtlich der „Abgleichergebnisse“ bzw. „Trefferfälle“ aus dem vom Gesetzgeber vorgesehenen Zusammenführen aus Halbsatz 1.

Mindestens im Rahmen des Verarbeitens ermächtigt Art. 61 Abs. 1 Satz 1 BayPAG damit zu einer automatisierten und methodenoffenen Datenanalyse auch der zuvor zusammengeführten Daten.

Dementsprechend rekurriert der bayerische Gesetzgeber in der Gesetzesbegründung wiederholt explizit auf die Rechtsprechung des angerufenen Gerichts zur automatisierten Datenanalyse oder -auswertung,

vgl. LT-Drs. 19/1557, S. 13, 23 ff.

Er geht selbst davon aus, zumindest mit Art. 61a Abs. 1 Satz 1 BayPAG zu einem schwerwiegenden Grundrechtseingriff im Sinne des Datenanalyseurteils des angerufenen Gerichts zu ermächtigen und an die diesbezüglichen verfassungsrechtlichen Anforderungen gebunden zu sein,

vgl. LT-Drs. 19/1557, S. 23, 24.

Für die Annahme einer umfassenden, methodenoffenen Analysebefugnis spricht auch die Gesetzgebungshistorie. Der Gesetzgeber intendiert die Nutzung einer verfahrensübergreifenden Recherche- und Analyseplattform „zum regelbasierten und formatübergreifenden Abgleich“ und „zur Zusammenführung polizeiinterner Daten“,

vgl. LT-Drs. 19/1557, S. 1.

Dies fügt sich in die obenstehende Auslegung ein.

Für dieses Verständnis spricht systematisch zudem, dass ein einfacher „Abgleich“ von Daten bereits in Art. 61 BayPAG geregelt ist. Das „Zusammenführen“ und „Verarbeiten“ i.S.d. Art. 61a BayPAG muss also über den bloßen Vergleich von Daten auf Übereinstimmungen hinausgehen. Da auch der bloße Datenabgleich nach Art. 61 BayPAG (wie jede informationelle Maßnahme) der Gewinnung neuer Erkenntnisse dient, das Merkmal dort aber nicht genannt wird, lässt die Formulierung in Art. 61a Abs. 1 Satz 1 BayPAG darauf schließen, dass die Befugnis über einen einfachen Abgleich hinaus gehen soll, da die Erkenntnisse gerade durch komplexere Auswertungen auf automatisiertem Wege gewonnen werden sollen.

Auch der Ausschluss einer ausschließlich automatisierten Entscheidungsfindung im Einzelfall in Art. 61a Abs. 5 Nr. 1 und Nr. 2 BayPAG wäre unverständlich, wenn es sich nur um einen bloßen Abgleich von Daten handeln würde. Eine solche könnte nie zu einer automatisierten Entscheidungsfindung führen. Auch dem Ausschluss der Verwendung selbstlernender Systeme käme bei einer einfachen Such- und Abgleichfunktion keine wesentliche Bedeutung zu.

Schließlich zeigt auch der Sinn und Zweck des Gesetzes, dass durch die neue Befugnis der Einsatz der Software „VeRA“ gerechtfertigt und damit automatisierte Datenanalysen ermöglicht werden sollen. Art. 61a BayPAG wurde gerade als Rechtsgrundlage für die Software geschaffen, die als Analysesoftware eingesetzt wird,

> siehe die Begründung des Staatsministers für Inneres, Sport und Integration, Joachim Hermann, Bayerischer Landtag-Prot. 19/17 vom 25. April 2024, S. 1186; Bayerische Staatsregierung, Pressemitteilung „Herrmann: Landtag beschließt Änderungen im Polizeiaufgabengesetz“, 17. Juli 2024, https://www.bayern.de/herrmann-landtag-beschliesst-aenderungen-im-polizeiaufgabengesetz/; *Aulehner*, in: BeckOK PolR Bayern 25. Ed. 15.10.2024, PAG Art. 61a, Rn. 13.

Die aufgrund von Art. 61a BayPAG eingesetzte Software „VeRA“ basiert auf der Software Gotham des Anbieters Palantir, die die Verknüpfung und visuelle Aufbereitung der Daten ermöglicht. Auf Basis dieser Ergebnisse sollen durch polizeiliche Sachverarbeiter*innen Hypothesen erstellt und ggf. verifiziert bzw. falsifiziert werden können,

> vgl. LT-Drs. 18/22731, S. 6 ff.

Die Software wird vom Hersteller als „Operation System for Decision Making“ bezeichnet,

> siehe dazu die firmeneigene Website, abrufbar unter https://www.palantir.com/platforms/gotham/#a-section; ebenso im Werbevideo „Palantir Gotham for Defense Decision Making“ auf dem offiziellen YouTube-Kanal des Unternehmens Palantir, abrufbar unter https://www.youtube.com/watch?v=rxKghrZU5w8.

Gotham wird explizit damit beworben, dass es aus verschiedenen Datenquellen auch komplexe Bewertungen wie z.B. Prognosen möglicher Routen von Schiffen in Angriffsfällen abgeben sowie bestmögliche Reaktionsmittel durch eigene Infrastruktur ermitteln und empfehlen kann,

> so im Werbevideo „Palantir Gotham for Defense Decision Making" auf dem offiziellen YouTube-Kanal des Unternehmens Palantir, abrufbar unter https://www.youtube.com/watch?v=rxKghrZU5w8.

Die Software wird auch in Hessen („hessenDATA") und Nordrhein-Westfalen („DAR") zur Datenanalyse genutzt, „VeRA" ist mit diesen Softwares vergleichbar,

> so ausdrücklich der Staatsminister für Inneres, Sport und Integration, Joachim Hermann, Bayerischer Landtag-Prot. 19/17 vom 25. April 2024, S. 1186.

(2) Unzureichende gesetzliche Beschränkungen der Methode

Die im Gesetzeswortlaut vorgesehenen Beschränkungen in Art. 61a Abs. 4 Satz 3 (**(a)**) und Abs. 4 Nr. 1-3 BayPAG (**(b)**-**(d)**) genügen nicht, um das Eingriffsgewicht der vorgesehenen Datenanalyse zu verringern.

(a) Art. 61a Abs. 4 Satz 3 BayPAG

Art. 61a Abs. 4 Satz 3 BayPAG beschränkt die Anzeige der Ergebnisse zwar auf die mit Suchparametern übereinstimmenden Treffer. Dabei sind jedoch auch offene Suchen und Suchanfragen möglich, die sich zum Beispiel auf statistische Auffälligkeiten in der Datenmenge richten. Auch ist die Anzahl der Suchanfragen und Abgleichschritte nicht von vornherein begrenzt, sodass komplexe Analysen mit immer wieder aufeinander aufbauenden Suchanfragen möglich sind. Die einschränkende Wirkung ist vor diesem Hintergrund stark begrenzt.

Art. 61a Abs. 4 Satz 3 BayPAG hat nicht zur Folge, dass – wie in der Gesetzesbegründung angenommen – die Datenanalyse nur die systematische Erschließung vorhandener Datenbestände durch Suchfunktion ermögliche,

> vgl. LT-Drs. 19/1557, S. 23.

Der Gesetzeswortlaut selbst beschränkt den Einsatz der Datenanalysesoftware gerade nicht nur auf das Erschließen und Durchsuchen von Datenbeständen. Dies ergibt sich schon daraus, dass die Zusammenführung und weitere Verarbeitung gerade „zur Gewinnung neuer Erkenntnisse“ (Art. 61a Abs. 1 Satz 1 BayPAG) erfolgen soll. Darüber hinaus sind in Art. 61a BayPAG weder Leistung noch Charakteristik oder Funktionsweisen der eingesetzten Algorithmen eingeschränkt. Insbesondere ist damit auf Basis der Suchverläufe auch komplexes Data-Mining und eigenständige automatisierte Risikobewertung auf Basis der Daten möglich.

(b) Art. 61a Abs. 5 Nr. 1 BayPAG

Art. 61a. Abs. 5 Nr. 1 BayPAG untersagt bei der Anwendung von Maßnahmen nach Absatz 1 und Absatz 2 eine automatisierte Entscheidungsfindung im Sinne von Art. 11 JI-Richtlinie. Art. 11 Abs. 1 verpflichtet die Mitgliedsstaaten, „ausschließlich auf einer automatischen Verarbeitung beruhende Entscheidungen – einschließlich Profiling –“ zu verbieten, „die eine nachteilige Rechtsfolge für die betroffene Person haben oder sie erheblich beeinträchtigen“.

Art. 61a. Abs. 5 Nr. 1 BayPAG beschränkt die zulässigen Analysemethoden nur in geringem Maße, da er eine Berücksichtigung automatisierter Bewertungsergebnisse und Profiling im Rahmen polizeilicher Maßnahmeanordnungen gerade nicht vollständig ausschließt (dazu **(aa)**). Zudem genügt der Ausschluss nicht den verfassungsrechtlichen Anforderungen an Bestimmtheit und Normenklarheit (dazu **(bb)**).

(aa) Geringe Beschränkung der Methode durch den Ausschluss

Gemäß Art. 61a Abs. 5 Nr. 1 BayPAG i.V.m. Art. 11 Abs. 1 Halbsatz 2 JI-Richtlinie sind nur vollautomatisierte Entscheidungen und Maßnahmen ausgeschlossen, die ohne jegliche menschliche Entscheidung oder Mitwirkung ergehen bzw. ergriffen werden. Dies gilt auch für Profiling im Sinne von Art. 3 Nr. 4 der JI-Richtlinie.

Dem Wortlaut nach kann bei weitestgehend automatisierten Analyse- und Bewertungsvorgängen schon nur eine minimale menschliche Mitwirkung dazu führen, dass die Maßnahme zulässig ist.

Es ist mithin möglich, durch eine Vielzahl von Suchverläufen zu Analyseergebnissen durch automatisierte Bewertungen zu gelangen und diese ohne weitere Ermittlung oder Analyse von Mitarbeiter*innen zur Grundlage für Entscheidungen zu machen, solange eine nicht näher spezifizierte auch nur geringfügige Kontrolle erfolgt.

Eine solche Auslegung des Art. 61a Abs. 5 Nr. 1 BayPAG lässt auch die Gesetzesbegründung erkennen:

> „Insbesondere durch den Ausschluss selbstlernender Systeme und der automatisierten **Entscheidungsfindung ohne die Kontrolle durch einen Mitarbeiter** wird das Risiko des Einzelnen, aufgrund von „Zufallstreffern" Betroffener einer weiteren polizeilichen Maßnahme zu werden, erheblich gemindert."
>
> vgl. LT-Drs. 19/1557, S. 29 [Hervorhebungen durch Unterzeichner].

In der Literatur zu Art. 22 DSGVO, der parallel zu Art. 11 der JI-Richtlinie ein Verbot automatisierter Entscheidungsfindung regelt, wird der Ausschluss unterschiedlich weit ausgelegt.

Teils wird eine ausschließliche Automatisierung bzw. „kein Dazwischentreten eines Menschen" auch dann angenommen, wenn zwar eine menschliche Kontrolle erfolgt, diese aber keine inhaltliche Kontrolle darstellt, die die automatisierte Bewertung in eine eigene Entscheidung eines Menschen übersetzt. Bloß formale Nachbearbeitungen könnten nicht genügen,

> *von Lewinski*, in: BeckOK DatenschutzR, 52. Ed. 1.8.2025, DS-GVO, Art. 22, Rn. 23, 25 m.w.N.; *Martini,* in: Paal/Pauly, DS-GVO, 3. Aufl. 2021, Art. 22, Rn. 17b; *Scholz,* in: Simitis/Hornung/Spiecker, Datenschutzrecht, 2. Aufl. 2025, DS-GVO, Art. 22, Rn. 29; *Taeger,* in: Gabel/Taeger, 4. Aufl. 2022, DS-GVO Art. 22 Rn. 29.

Ebenso sei von einer automatisierten Entscheidungsfindung auszugehen, wenn der überprüfenden Person kein Entscheidungsspielraum zukomme,

von Lewinski, in: BeckOK DatenschutzR, 52. Ed. 1.8.2025 DS-GVO, Art. 22, Rn. 25 m.w.N.; *Martini,* in: Paal/Pauly, DS-GVO, 3. Aufl. 2021, Art. 22, Rn. 19; *Scholz,* in: Simitis/Hornung/Spiecker, Datenschutzrecht, 2. Aufl. 2025, DS-GVO Art. 22, Rn. 30.

Teils wird zusätzlich gefordert, dass die Person mit entsprechender Entscheidungskompetenz ausgestattet und instruiert sein muss und zu derartigen Entscheidungen befugt ist,

Schulz, in: Gola/Heckmann, DS-GVO, 3. Aufl. 2022, Art. 22, Rn. 15; *Martini,* in: Paal/Pauly, DS-GVO, 3. Aufl. 2021, Art. 22, Rn. 18 f.; *Scholz,* in: Simitis/Hornung/Spiecker, Datenschutzrecht, 2. Aufl. 2025, DS-GVO, Art. 22, Rn. 33; *Helfrich*, in: Sydow/Marsch DS-GVO/BDSG, 3. Aufl. 2022, DSGVO, Art. 22, Rn. 43.

Andererseits wird für ausreichend erachtet, dass die Entscheidung „am Ende von einem Menschen getroffen wird", also wenn die automatisierte Entscheidung nur Vorschläge für eine von Menschen vorzunehmende und inhaltlich zu verantwortende Entscheidung bereitstellt,

Hladjk, in: Ehmann/Selmayr, DSGVO, 3. Aufl. 2024, Art. 22, Rn. 6; *Buchner,* in: Kühling/Buchner, DS-GVO, 4. Aufl. 2024, Art. 22, Rn. 15.

Auch wird vertreten, ein Mensch müsse eine Wahl zwischen mindestens zwei Optionen treffen und hierzu eigenständige Kriterien anwenden,

Helfrich, in: Sydow/Marsch DS-GVO/BDSG, 3. Aufl. 2022, DSGVO, Art. 22, Rn. 43.

Einigkeit besteht jedoch darüber, dass eine Entscheidung dann nicht unter Art. 22 DSGVO fällt, wenn sie nur zum Teil oder nur überwiegend auf einer maschinellen Bewertung beruht,

Schulz, in: Gola/Heckmann, DS-GVO, 3. Aufl. 2022 Art. 22, Rn. 11; *Buchner,* in: Kühling/Buchner, DS-GVO, 4. Aufl. 2024, Art. 22, Rn. 14; *Scholz,* in: Simitis/Hornung/Spiecker, Datenschutzrecht, 2. Aufl. 2025, DS-GVO Art. 22, Rn. 31; *Helfrich*, in: Sydow/Marsch DS-GVO/BDSG, 3. Aufl. 2022, DSGVO, Art. 22, Rn. 42; *Hladjk,* in: Ehmann/Selmayr, DSGVO, 3. Aufl. 2024, Art. 22, Rn. 6.

So könnten nicht ausschließlich automatisierte Entscheidungen (z.B. als Grundlage oder zur Vorbereitung) auch Profiling und andere automatisierte Entscheidungen beinhalten,

> *Hladjk,* in: Ehmann/Selmayr, DSGVO, 3. Aufl. 2024, Art. 22, Rn. 6; *Schulz,* in: Gola/Heckmann, DS-GVO, 3. Aufl. 2022 Art. 22, Rn. 11; *Scholz,* in: Simitis/Hornung/Spiecker, Datenschutzrecht, 2. Aufl. 2025, DS-GVO Art. 22, Rn. 31.

Es dürfen sowohl automatisierte Entscheidungsvorschläge wie z.B. automatisierte Vorauswahlen von Personen in die Entscheidung einbezogen werden, solange es sich lediglich um eine Entscheidungshilfe handelt,

> *Scholz,* in: Simitis/Hornung/Spiecker, Datenschutzrecht, 2. Aufl. 2025, DS-GVO Art. 22, Rn. 31.

Da polizeiliche Maßnahmen eine menschliche Anordnung erfordern und im Einzelfall ein Ermessen sowie ggf. weitere Anordnungsvoraussetzungen vorsehen, kommt dem Ausschluss bei dieser Auslegung kaum begrenzende Bedeutung zu.

Eine weitergehende Einschränkung des Ausschlusses ergibt sich auch nicht aus der Rechtsprechung des Gerichtshofs der Europäischen Union (EuGH) zur automatisierten Entscheidungsfindung in Art. 22 DSGVO, der wie Art. 11 der JI-Richtlinie ein Verbot automatisierter Entscheidungsfindung regelt,

> EuGH, Urteil vom 7. Dezember 2023, C-634/21 (Schufa Holding AG), Rn. 42 ff., 52.

Der EuGH beantwortet dabei die Vorlagefrage wie folgt:

> Art. 22 Abs. 1 […] ist dahin auszulegen, dass eine „automatisierte Entscheidung im Einzelfall“ im Sinne dieser Bestimmung vorliegt, wenn ein auf **personenbezogene Daten zu einer Person gestützter Wahrscheinlichkeitswert** in Bezug auf deren Fähigkeit zur Erfüllung künftiger Zahlungsverpflichtungen durch eine Wirtschaftsauskunftei **automatisiert erstellt** wird, **sofern** von diesem **Wahr-**

> **scheinlichkeitswert maßgeblich abhängt, ob** ein Dritter, dem dieser Wahrscheinlichkeitswert übermittelt wird, ein Vertragsverhältnis mit dieser Person begründet, durchführt oder beendet.
>
> EuGH, Urteil vom 7. Dezember 2023, C-634/21 (Schufa Holding AG), Rn. 72 [Hervorhebungen durch Unterzeichner].

Im Rahmen der Entscheidung über die Berücksichtigung eines automatisiert erstellten Schufa-Scores eines Drittanbieters als maßgebliches Kriterium für eine Kreditvergabe legt der EuGH den Begriff der „Entscheidung" zwar weit aus. Entscheidung sind danach nicht nur Handlungen, die rechtliche Wirkung gegenüber betroffenen Personen entfalten, sondern auch solche Handlungen, die in ähnlicher Weise Personen erheblich beeinträchtigen,

> EuGH, Urteil vom 7. Dezember 2023, C-634/21 (Schufa Holding AG), Rn. 43 ff.

Dabei kann eine Entscheidung auch mehrere Handlungen umfassen,

> EuGH, Urteil vom 7. Dezember 2023, C-634/21 (Schufa Holding AG), Rn. 46.

Auch beruhte die Entscheidung „ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling", da die Profiling-Definition des Art. 4 Nr. 4 der DSGVO (ebenso in § 3 Nr. 4 JI-Richtlinie) erfüllt ist,

> EuGH, Urteil vom 7. Dezember 2023, C-634/21 (Schufa Holding AG), Rn. 47.

Daher greift das Verbot nach Art. 22 DSGVO bereits für die Ermittlung eines Scores zur Kreditwürdigkeit einer Person auch dann, wenn die automatisierte Entscheidungsfindung nur als vorbereitende Handlung erfolgt, solange die weitere Entscheidung „maßgeblich" von dieser geleitet ist und auch dann, wenn die automatisierte Entscheidungsfindung durch einen Dritten durchgeführt wird. Das im Vorfeld von einem Dritten durchgeführte Profiling ist in diesem Falle ebenfalls eine Entscheidung im Sinne des Art. 22 DSGVO,

EuGH, Urteil vom 7. Dezember 2023, C-634/21 (Schufa Holding AG), Rn. 46, 61 ff.

Es ist jedoch bereits unklar, ob diese Maßstäbe auf das in Art. 11 der JI-Richtlinie geregelte grundsätzliche Verbot ohne weiteres übertragen werden können.

Jedenfalls kann aus der Entscheidung zu einem Kreditwürdigkeits-Scoring, dessen Maßgeblichkeit für die Entscheidung für die Kreditvergabe für den EuGH feststand, nicht gefolgert werden, automatisierte Scoring- oder Profiling-Entscheidungen seien nach Art. 22 Abs. 1 DSGVO bzw. Art. 11 Abs. 1 JI-Richtlinie generell unzulässig,

so auch für Schufa-Scorings *Marsch/Kratz*, NJW 2024, 392 (393).

Es ist nicht durch Art. 61a Abs. 5 Nr. 1 BayPAG i.V.m. Art. 11 Abs. 1 JI-Richtlinie ausgeschlossen, dass Polizist*innen über Gefahrenabwehrmaßnahmen entscheiden und ihrer Entscheidung dabei eine automatisierte Profiling-Entscheidung zugrunde legen.

Dies ergibt sich schon daraus, dass Art. 11 Abs. 3 der JI-Richtlinie ausdrücklich bestimmte Formen des Profilings ausschließt, sodass im Rückschluss nach Art. 11 Abs. 1 gerade auch andere Profiling-Entscheidungen zulässig sind,

Schantz/Wolff, Das neue Datenschutzrecht, 1. Aufl. 2017, Rn. 753; zu Art. 22 DSGVO ausdrücklich: *Hladjk* in: Ehmann/Selmayr, DSGVO, 3. Aufl. 2024, Art. 22, Rn. 6.

Darüber hinaus hat der EuGH in seiner Entscheidung keine Vorgaben zu den Tatbestandsmerkmalen „ausschließlich auf automatischer Verarbeitung beruhende“ bzw. „Profiling“ und „die eine nachteilige Rechtsfolge für die betroffene Person hat oder sie erheblich benachteiligt“ des Art. 11 der JI-Richtlinie gemacht, da das Vorliegen dieser Voraussetzungen seiner Auffassung nach feststand,

EuGH, Urteil vom 7. Dezember 2023, C-634/21 (Schufa Holding AG), Rn. 47 f., 49 f. ohne tiefergehende Auseinandersetzung; in der Entscheidung des EuGH, Urteil vom 27. Februar 2025, C-203/22, Rn. 38,

> 46, 66 geht der EuGH ohne weitere Subsumtion von einer automatisierten Entscheidungsfindung im Sinne des Art. 22 Abs. 1 DSGVO aus, da eine Maßgeblichkeit der automatisierten Schufa-Score-Entscheidung für die Kreditvergabe feststand.

In dem vom EuGH entschiedenen Fall wurden bei einem geringen Wahrscheinlichkeitswert Online-Kreditanträge oder Online-Einstellungsanträge in nahezu allen Fällen abgelehnt,

> EuGH, Urteil vom 7. Dezember 2023, C-634/21 (Schufa Holding AG), Rn. 45, 48.

Der EuGH hat eine Unzulässigkeit einer automatisierten Berechnung eines Wahrscheinlichkeitswerts und damit einer Profiling-Entscheidung in diesem Falle nur deshalb angenommen, weil eindeutig feststand, dass die weitere Entscheidung über die Kreditvergabe „maßgeblich von diesem [durch Profiling im Sinne von Art. 4 Nr. 4 DSGVO ermittelten Wert] geleitet wird“,

> EuGH, Urteil vom 7. Dezember 2023, C-634/21 (Schufa Holding AG), Rn. 46 ff., 48, 61, 62.

Diese Anforderung beschränkt das Verbot der automatisierten Entscheidungsfindung erheblich, da die Maßgeblichkeit im Einzelfall festgestellt sein muss,

> *Matsch/Kratz*, NJW 2024, 392 (393); *Hense*, RDi 2024, 192 (194 f.); *Ringle* GRUR-Prax 2024, 107 (Praxishinweis).

Eine automatisierte Datenanalyse ist somit zwar als „ausschließlich auf einer automatisierten Verarbeitung – einschließlich Profiling“ beruhend anzusehen, wenn sie die Profiling-Definition des Art. 3 Nr. 4 JI-Richtlinie erfüllt. Auch hier stellt sich aber die Frage, wie viel menschliche Mitwirkung im Rahmen der „automatisierten Verarbeitung“ dazu führt, dass es sich nicht um Profiling handelt.

Dass das Ergebnis einer Datenanalyse aber in jedem Falle für die weitere Entscheidung formal rechtlich verbindlich und diese damit „maßgeblich“ von einer Bewertung des Risikos durch die Analysesoftware „geleitet“ ist,

wird sich schon aufgrund der bestehenden Ermessensspielräume und weiten Entscheidungsgrundlage der anordnenden Polizist*innen schwerlich nachweisen lassen. Damit wird es regelmäßig an der Maßgeblichkeit der Profiling-Entscheidung im Vorfeld, die für den Ausschluss notwendig wäre, fehlen.

Eine solche Maßgeblichkeit ist jedenfalls für solche Maßnahmen abzulehnen, die unter einem Richtervorbehalt stehen, da hier davon auszugehen ist, dass durch die divergierenden Personen bei Analysedurchführung und Anordnung der Maßnahmen durch Gerichtsbeschluss eine Maßgeblichkeit der automatisierten Entscheidung nicht gegeben ist. Eine gerichtliche Entscheidung wird mangels gesetzlicher Vorgaben nicht maßgeblich von der Analyse geleitet sein.

Damit ist nicht generell ausgeschlossen, dass automatisierte Profiling-Entscheidungen im Vorfeld polizeilicher Maßnahmen durchgeführt werden können. Diese sind vielmehr zulässig, solange die aus mehreren Handlungen bestehende Entscheidung nicht insgesamt maßgeblich auf der automatischen Verarbeitung beruht oder von dem Profiling nicht selbst unmittelbar Beeinträchtigungen ausgehen.

Höhere Anforderungen an die Qualität menschlicher Kontrolle oder menschlicher Entscheidungsfindung bzw. an die Maßgeblichkeit des Profilings im Vorfeld hat der EuGH nicht aufgestellt.

Aus diesem Grund bleibt es für diese Tatbestandsmerkmale beim Wortlaut des Art. 11 Abs. 1 JI-Richtlinie: Nach diesem ist nur eine unmittelbar und ausschließlich auf der automatisierten Verarbeitung beruhende Entscheidung bzw. Profiling ausgeschlossen, von der die Anordnung einer rechtlich oder tatsächlich belastenden Maßnahme bzw. Endentscheidung „geleitet“ ist.

Gerade bei der Nutzung von automatischen Datenverarbeitungs- und Datenanalyseanwendungen im Vorfeld besteht zusätzlich das Risiko, dass für die Entscheidung, ob gegen eine Person Gefahrenabwehrmaßnahmen angeordnet werden, die Ergebnisse der Analysesoftware zwar nicht rechtlich verbindlich und damit nicht formal maßgeblich sind, sondern auch andere

Gesichtspunkte und Bewertungen in die Entscheidungsfindung einfließen, Polizist*innen dem Ergebnis einer Datenanalyse aber unterbewusst eine höhere Bedeutung und Aussagekraft beimessen und dieses überwerten (sogenannter automation bias),

> zum Begriff näher *Ruschemeier*, in: Proceedings of the Weizenbaum Conference 2023: AI, Big Data, Social Media, and People on the Move, 2023, S. 1 (4); *Schiemer*, Automation Bias einfach erklärt: Warum wir automatisierten Systemen zu sehr vertrauen, biases.de, abrufbar unter https://biases.de/automation-bias/.

So kann es gerade in Fällen der entscheidungsvorbereitenden Datenverarbeitung bzw. des Profilings im Vorfeld einer Entscheidung, die nicht nach Art. 61a Abs. 5 Nr. 1 BayPAG ausgeschlossen sind, zu einer faktischen Ausrichtung von Entscheidungen an den Profiling-Ergebnissen kommen. Auch diesem Risiko begegnet der Ausschluss nicht, obwohl Regelungen dazu im grundrechtssensiblen Bereich des Gefahrenabwehrrechts notwendig wären,

> *Ruschemeier*, in: Proceedings of the Weizenbaum Conference 2023: AI, Big Data, Social Media, and People on the Move, 2023, S. 1 (8).

(bb) Unzureichende Bestimmtheit und Normenklarheit des Ausschlusses

Dem Ausschluss kommt im Übrigen bereits keine ausreichende Einschränkungswirkung zu, da er zu unbestimmt und jedenfalls nicht ausreichend normenklar formuliert ist. Die aufgrund der Heimlichkeit der Datenanalyse erforderlichen hohen verfassungsrechtlichen Anforderungen (siehe dazu **D.I.1.b.bb.aaa.**) sind nicht gewahrt.

Die soeben dargestellten Auslegungsunklarheiten im Hinblick auf vollständige Automatisierung, Entscheidungsfindung und Rechtsfolge bzw. nachteilige Wirkung der Entscheidung lassen bereits für die normanwendenden Behörden nicht zu, die Reichweite des Ausschlusses für die Praxis zu erkennen.

Zwar sind Verweisungen auf Normen nicht grundsätzlich abträglich für die Bestimmtheit und Normenklarheit. Unter Anwendung der für Verweisungen geltenden verfassungsrechtlichen Maßstäbe liegt hier jedoch eine Verweisung vor, durch die der Ausschluss nach Art. 61a Abs. 5 Nr. 1 BayPAG seine Klarheit verliert und in der Praxis zu übermäßigen Schwierigkeiten bei der Anwendung führt.

Dies folgt formal schon daraus, dass es sich bei der Verweisung des Art. 61a Abs. 5 Nr. 1 BayPAG um eine dynamische Verweisung auf Art. 11 JI-Richtlinie und damit auf die Norm eines anderen Gesetzgebers handelt. Verweise auf EU-Recht sind dabei unter den gleichen Voraussetzungen wie andere dynamische Verweisungen nur in dem Rahmen zulässig, den die Prinzipien der Rechtsstaatlichkeit, der Demokratie und der Bundesstaatlichkeit setzen,

BVerfGE 143, 38 (61 f. Rn. 58 f.).

Vorliegend lagert der Gesetzgeber die Entscheidung über die Reichweite seines Ausschlusses im Rahmen des dynamischen Verweises vollständig auf den EU-Gesetzgeber aus. Änderungen des Unionsrechts wirken sich somit unmittelbar auf die Reichweite des Methodenausschlusses des Art. 61a Abs. 5 Nr. 1 BayPAG aus. Da der Gesetzgeber diesen gerade normiert, um das starke Eingriffsgewicht automatisierter Datenanalysen zu verringern, genügt er mit dieser Auslagerung nicht seiner originär eigenen Abwägungsverpflichtung zum Schutz der Grundrechte, insbesondere der informationellen Selbstbestimmung. Schon dies spricht für eine mangelnde Bestimmtheit der Norm.

Selbst bei einer Auslegung des Verweises als statisch auf die im Zeitpunkt des Inkrafttretens geltende Fassung der Richtlinie ist darüber hinaus nicht erkennbar, wie weit die Inbezugnahme des Art. 11 JI-Richtlinie in Art. 61a Abs. 5 Nr. 1 BayPAG reicht.

Art. 11 JI-Richtlinie regelt in Absatz 1 Halbsatz 1 in zwei Untersatzteilen ein Verbot für automatisierte Entscheidungsfindung im Einzelfall. Eine Ausnahme besteht nach Absatz 1 Halbsatz 2, wenn die Entscheidungsfindung „nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, dem der

Verantwortliche unterliegt und das geeignete Garantien für die Rechte und Freiheiten der betroffenen Person bietet, zumindest aber das Recht auf persönliches Eingreifen seitens des Verantwortlichen, erlaubt“ ist. Art. 11 Abs. 2 der Richtlinie untersagt, dass Entscheidungen nach Abs. 1 auf Daten nach Art. 10 DSGVO beruhen. Art. 11 Abs. 3 verbietet Profiling, das zur Folge hat, dass natürliche Personen auf Grundlagen von Daten nach Art. 10 DSGVO diskriminiert werden.

Die Reichweite des Ausschlusses hängt schon davon ab, ob für die „automatisierte Entscheidungsfindung im Sinn von Art. 11“ der JI-Richtlinie nur der erste Teil von Art. 11 Abs. 1 Halbsatz 1 („eine ausschließlich auf einer automatischen Verarbeitung beruhende Entscheidung – einschließlich Profiling –") oder auch auf die weitere Anforderung („die eine nachteilige Rechtsfolge für die betroffene Person hat oder sie erheblich beeinträchtigt“) in Bezug genommen sein soll. Art. 11 Abs. 1 JI-Richtlinie enthält keine klar begrenzte Legaldefinition, sondern eine Umschreibung der automatisierten Entscheidungsfindung, deren Grenzen im Wortlaut nicht klar sind.

Ebenso ist durch den pauschalen Verweis auf den gesamten Art. 11 JI-Richtlinie nicht klar, ob auch der übrige Art. 11 Abs. 1 oder sogar der gesamte Art. 11 JI-Richtlinie einbezogen werden sollen.

Unklar ist zum einen, ob auch die Einschränkung einbeziehbarer personenbezogener Daten in Art. 11 Abs. 2 und das Verbot diskriminierenden Profilings nach Art. 11 Abs. 3 JI-Richtlinie von der Verweisung mit umfasst sind. Zum anderen ist der pauschale Verweis auf Art. 11 JI-Richtlinie bereits nicht ausreichend bestimmt. In Absatz 1 Halbsatz 2 stellt der Richtliniengeber das Verbot der automatisierten Entscheidungsfindung nämlich gerade unter die Einschränkung einer Gestattung der Entscheidungsfindung durch Recht der Mitgliedsstaaten. Der Verweis des nationalen Rechts auf die Öffnungsklausel wäre insoweit bereits zirkelschlüssig.

Auch ist allein durch den Verweis auf Art. 11 JI-Richtlinie mangels weiterer Vorgaben nicht festgelegt, inwieweit automatisiertes Profiling im Vorfeld oder zur Vorbereitung polizeilicher Maßnahmen erfolgen darf. Es ist nicht klar ersichtlich, unter welchen Voraussetzungen auch rein automatisierte

Entscheidungen im Vorfeld bereits vollständig ausgeschlossen sein sollen. Insbesondere bestehen – selbst bei Heranziehen der dargestellten Rechtsprechung des EuGHs zu Art. 22 DSGVO – keine Anhaltspunkte, wann von einer vollständigen Automatisierung der Entscheidung auszugehen ist bzw. bei wie viel menschlicher Mitwirkung eine solche nicht mehr gegeben ist. Darüber hinaus ist auch unklar, wann eine automatisierte Datenanalyse, beispielsweise durch Profiling, so maßgeblich für eine Entscheidung ist, dass sie zu einer negativen Rechtsfolge oder sonstigen belastenden Wirkung führt.

Jedenfalls ist Art. 61a Abs. 5 Nr. 2 BayPAG nicht ausreichend normenklar, da sich seine Reichweite für Bürger*innen nicht klar aus der Norm selbst ergibt. Insoweit geht die inhaltliche Verständlichkeit der Norm verloren. Für Bürger*innen wie die Beschwerdeführer*innen ist anhand der gesetzlichen Regelung des Ausschlusses in Art. 61a Abs. 5 Nr. 1 BayPAG nicht ausreichend klar erkennbar, dass sie für die Reichweite des Ausschlusses einer Methode nicht nur die direkt in Bezug genommene JI-Richtlinie, sondern – so von einer Übertragbarkeit und einer einschränkenden Wirkung ausgegangen wird – auch das inhaltlich übereinstimmende Methodenverbot des Art. 22 Abs. 1 DSGVO und die dazu ergangene EuGH-Rechtsprechung in den Blick nehmen müssen. Es handelt sich um eine lange, gestaffelte und nicht aus der Norm selbst nachvollziehbare Verweisungskette, die die Verständlichkeit der Regelung aufhebt. Die Parallelität von Art. 11 JI-Richtlinie und Art. 22 DSGVO ist selbst für Jurist*innen ohne besondere Kenntnisse im Sicherheitsrecht mangels Bekanntheit der JI-Richtlinie nicht offensichtlich. Jedenfalls für nicht juristisch ausgebildete Menschen ist die Verweisungskette auf Art. 22 DSGVO und damit auf die dazu existierende EuGH-Rechtsprechung nicht mehr nachvollziehbar, da sie sich nicht aus der Norm ergibt. Für Bürger*innen bleibt es damit bei dem pauschalen Verweis auf Art. 11 JI-Richtlinie mit den bereits dargestellten Argumenten. Schon diese Verweisungskette selbst führt insoweit zur fehlenden Normenklarheit.

Selbst wenn diese Rechtsquellen als relevant identifiziert werden, ist deren Anwendbarkeit bzw. Übertragbarkeit jedenfalls für Bürger*innen, die ihr

Verhalten an der Rechtgrundlage ausrichten wollen, aber nicht ohne weiteres ersichtlich. Selbst bei Übertragung der vom EuGH für die DSGVO aufgestellten Grundsätze sind nämlich wesentliche Auslegungsfragen des Verbotes weiterhin ungeklärt (siehe soeben) und werden durch Art. 61a Abs. 5 Nr. 1 BayPAG auch nicht präzisiert. Dieser sieht insbesondere keine Vorgaben dazu vor, welche anderen Gesichtspunkte neben einer Maßnahme nach Art. 61a BayPAG auch in die Entscheidungen einfließen müssen, um sicherzustellen, dass die Datenauswertung nach Art. 61a BayPAG für Folgeanordnungen nicht maßgeblich ist. Gerade im Hinblick auf polizeiliches Profiling durch automatisierte Datenanalysen im Vorfeld einer Maßnahmeanordnung ist für Bürger*innen nicht erkennbar, in welchem Umfang diese zulässig sein sollen. Der Norm kann gerade nicht entnommen werden, dass Ergebnisse aus automatisiertem Profiling durch hochkomplexe Software nicht in die Entscheidungen über polizeiliche Maßnahmen einfließen können.

(c) Art. 61a Abs. 5 Nr. 2 BayPAG

Das Eingriffsgewicht ist ebenfalls nicht ausreichend durch gesetzliche Einschränkungen gemindert, da Art. 61a Abs. 5 Nr. 2 BayPAG den Einsatz von Künstlicher Intelligenz (KI) nicht vollständig ausschließt.

Das angerufene Gericht sieht beim Einsatz von KI im Rahmen einer automatisierten Datenanalyse das Risiko, dass sich die algorithmischen Systeme im Verlauf des maschinellen Lernprozesses immer mehr von der ursprünglichen menschlichen Programmierung lösen und so maschinelle Lernprozesse und Ergebnisse der Anwendungen immer schwerer nachvollziehbar werden,

BVerfGE 165, 363 (408 Rn. 100).

Zwar wird für die Zusammenführung und Verarbeitung gemäß Art. 61a Abs. 5 Nr. 2 BayPAG die Verwendung selbstlernender Systeme verboten.

Der Landesgesetzesgeber beabsichtigt durch die Regelung auszuschließen, dass die vom angerufenen Gericht benannten Gefahren eintreten,

vgl. LT-Drs. 19/1557, S. 29.

Dieser Ausschluss ist insoweit als positiv zu bewerten und schränkt in diesem Punkt das Eingriffsgewicht ein, da die Software mit den polizeilichen Daten nicht weiter lernen und sich nicht von der programmierten Weise fortentwickeln darf.

Trotzdem kann dieser Ausschluss das Eingriffsgewicht insgesamt nicht hinreichend reduzieren.

Der Ausschluss der Verwendung selbstlernender Systeme in Art. 61 Abs. 5 Nr. 2 BayPAG begrenzt erstens nur unzureichend, da die Verwendung von KI nur im Rahmen der „Zusammenführung" und „Verarbeitung" und damit der Analyse selbst ausgeschlossen ist. Es ist mithin weiterhin möglich, für die Analyse eine Software einzusetzen, die mit Hilfe von selbstlernenden Systemen entwickelt wurde. Der Ausschluss verhindert nur, dass die Algorithmen während des Analysebetriebes „weiterlernen". Dennoch können durch KI trainierte und geschaffene, hochkomplexe Analysemethoden zum Einsatz kommen,

so auch zu dem Gesetzentwurf, der, bis auf kleinste Änderungen, der nun geltenden Regelung entspricht *Petri*, Stellungnahme zum Fragenkatalog im Rahmen der Anhörung des Ausschusses für Kommunale Fragen, Innere Sicherheit und Sport zum Gesetzentwurf zur Änderung des Polizeiaufgabengesetzes und weiterer Rechtsvorschriften am 16. Mai 2024 – **Anlage 11**, S. 17 f.

Zweitens gehen auch von komplexen deterministischen Systemen, deren Analysefunktionen sich nicht weiter verändern können, Risiken aus, da auch hier Analysevorgänge wegen ihrer Komplexität schwer nachvollziehbar sein können,

BVerfGE 165, 336 (409 Rn. 101).

Dies gilt gerade, wenn KI in der Vorprogrammierung der Software zum Einsatz kommen kann, da dann nicht nachvollziehbare Algorithmen entstehen, sodass sich die Gefahren gleichermaßen verwirklichen.

Grundsätzlich gliedert sich der Lernzyklus eines selbstlernenden Systems in die Phase der Datenerhebung und des Aufbereitens, die Phase der Modellableitung und des Lernvorgangs sowie die Anwendungsphase,

> *Hüger*, Künstliche Intelligenz und Diskriminierung, 2023, S. 55 ff., insb. 57 f. m.w.N.; *Tinhofer*, DRdA 1a/2022, 170 (172 ff.).

Während einige Trainingsmethoden mit Abschluss der Trainingsphase ein finales, starres Modell erzeugen, ermöglichen andere Trainingstechniken eine stetige Selbstanpassung des Systems auf Grundlage einer sich ständig verändernden Fallbasis, sodass eine klare Trennung in Trainings- und Anwendungsphase nicht mehr möglich ist,

> *Hüger*, Künstliche Intelligenz und Diskriminierung, 2023, S. 61 m.w.N.

Auch wenn eine Selbstanpassung des Systems in der Anwendungsphase ausgeschlossen wäre, würden sich die Gefahren des Einsatzes lernfähiger Systeme dann lediglich in den Bereich der Vorprogrammierung verlagern. Auch hier können sich diskriminierende Muster herausbilden, die dann in der Anwendung fortwirken, da die zentralen technischen Ursachen algorithmenbasierter Diskriminierungen auf der Ebene der Trainingsdaten zu verorten sind,

> *Hüger*, Künstliche Intelligenz und Diskriminierung, 2023, S. 113 m.w.N.; *Spiecker/Towfigh*, Automatisch* Benachteiligt Das Allgemeine Gleichbehandlungsgesetz und der Schutz vor Diskriminierung durch algorithmische Entscheidungssysteme, 2023, S. 12; *Zuiderveen Borgesius,* Discrimination, Artificial Intelligence and Algorithmic Decision Making, 2018, S. 17.

Aber auch der Lernvorgang birgt Diskriminierungsrisiken, etwa bei der Bestimmung der Zielvariablen für den Modellierungsprozess. Im Modellierungsprozess selbst verstärken sich die im Trainingssatz vorhandenen diskriminierenden Verzerrungen. In der Anwendungsphase kommt es dann zu Bestätigungsverzerrungen durch Feedback-Schleifen,

> vgl. *Hüger*, Künstliche Intelligenz und Diskriminierung, 2023, S. 120 ff. m.w.N.; *Lauscher/Legner*, ZfDR 2022, 367 (372).

Zwar führt die Gesetzesbegründung als weitere Beschränkung an, durch Art. 61a Abs. 5 Nr. 2 BayPAG seien

> „zur Senkung des Eingriffsgewichts ausschließlich automatisiert wiederholte Abgleichschritte zur Verknüpfung der Abgleichergebnisse mit weiteren Datenbeständen ausgenommen“,
>
> vgl. LT-Drs. 19/1557, S. 29.

Diese Auslegung geht jedoch über das vorgesehene Verbot der Verwendung selbstlernender Systeme hinaus und findet keine Entsprechung im Gesetzeswortlaut. Sie kann daher keine Einschränkung des Eingriffsgewichts zur Folge haben.

Art. 61a Abs. 5 Nr. 2 BayPAG beschränkt die Methoden damit gerade nicht auf ausschließlich menschlich programmierte und trainierte Software und Algorithmen, deren Funktionsweise und Analysevorgänge transparent und nachvollziehbar sind.

Damit ist gerade nicht ausgeschlossen, dass die Polizei sogenannte predictive-policing-Systeme einsetzt und eine auf algorithmischer Bewertung basierende Risikoanalyse und Gefahrenprognose durchführt, solange die Algorithmen in ihrer Funktionsweise nicht mehr „weiterlernen“ und im Zeitpunkt der Analyse determiniert sind,

> a.A. *Benamor*, BayVBl 2025, 44 (48).

Dies gilt insbesondere für die in Bayern eingesetzte und auf Palantir Gotham basierende Software „VeRA“.

Selbst wenn die Software im Rahmen ihrer Anwendung durch die bayerische Polizei wegen Art. 61a Abs. 5 Nr. 2 BayPAG nicht mehr weiterlernt, kann diese aufgrund ihrer komplexen Algorithmen und der Programmierung durch KI ein

> „maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausga-

> ben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können“
>
> Art. 3 Nr. 1 Verordnung (EU) 2024/1689 (Verordnung über künstliche Intelligenz, im Folgenden KI-Verordnung)

und damit KI im Sinne der KI-Verordnung darstellen.

Gotham nutzt nach externer Einschätzung KI- und Machine-Learning-Algorithmen, um große und heterogene Datenmengen zu analysieren, Muster zu erkennen und Vorhersagen zu treffen,

> vgl. *Wolfenstein*, KI-Plattform Nachteile: Wesentliche Nachteile von Palantir für europäische Unternehmen und Institutionen, 18. April 2025, abrufbar unter https://xpert.digital/ki-plattform-nachteile/?utm_source=chatgpt.com.

Gotham wird zudem als KI-System beworben,

> so auf der offiziellen Webseite von Palantir erstens als „AI-driven combat superioriy“ unter https://www.palantir.com/platforms/gotham/ und zweitens unter „Unsere neue Plattform Künstliche - Intelligenz unserem kollektiven Willen unterwerfen - Ein Brief des CEO“, https://www.palantir.com/newsroom/letters/our-new-platform/de/.

So können zur Datenanalyse mit einer KI programmierte Systeme angewandt werden, die sich zwar während der Analyse selbst nicht mehr eigenständig verändern, die jedoch vergleichbar komplex und in ihrer Funktionsweise vergleichbar wenig nachvollziehbar für Anwendende und Betroffene sind. Diese stellen vorliegend eingriffsintensive Methoden dar, die weitere schützende Regelungen erforderlich machen,

> BVerfGE 165, 336 (409 Rn. 101).

(d) Art. 61a Abs. 5 Nr. 3 BayPAG

Art. 61 Abs. 5 Nr. 3 BayPAG begrenzt mit dem Ausschluss des automatisierten Abgleichs von personenbezogenen Daten lediglich den Umfang der in

die Verarbeitung einzubeziehenden Daten und nicht die Methoden der Datenverarbeitung (siehe oben **D.I.2.a.aa.bbb.**).

(3) Keine weitergehenden Einschränkungen der Methode

Die Gesetzesbegründung zu Art. 61a BayPAG geht von weitergehenden Beschränkungen der Analysemethode aus. Diese finden sich jedoch im Wortlaut der Norm nicht wieder. Gerade mit Blick auf die hohen Anforderungen an Bestimmtheit und Normenklarheit bei heimlichen Datenanalysen müssen Einschränkungen deutlichen Niederschlag im Normtext aufweisen. Den Beschränkungen kommt daher keine eingriffsmindernde Wirkung zu.

Die Eingriffsintensität der verwendeten Methoden wird insbesondere nicht dadurch beschränkt, dass die Gesetzesbegründung vorsieht, die Analyse der Daten und die Erlangung neuer Erkenntnisse aus dieser solle durch die ermittelnden Personen und nicht durch die Software erfolgen,

> vgl. LT-Drs. 19/1557, S. 23 f.

Die Bewertung der Daten erfolge nicht durch die automatisierte Datenzusammenführung, sondern durch Personal:

> „Besonders deutlich wird der Anwendungszweck der Maßnahme mit dem hiervon erfassten Ausschluss einer maschinellen Sachverhaltsbewertung. Durch Art. 61a soll der Rechercheaufwand reduziert und der zuständige Sachbearbeiter sich vorwiegend auf die eigentliche Analyse konzentrieren können. Eine Sachverhaltsbewertung durch eine Software findet gerade nicht statt. Die Bewertung muss folglich weiterhin der Mitarbeiter mit Hilfe eigener geistiger Fähigkeiten und Erfahrungswerte, ohne weitere Unterstützung des Systems, erledigen“,
>
> vgl. LT-Drs. 19/1557, S. 29.

Diese Einschränkung ist dem Gesetzeswortlaut selbst jedoch nicht zu entnehmen. Dieser lässt vielmehr gerade auch eine Analyse und Bewertung der Daten durch die Analysesoftware zu (siehe zum weiten Begriff der Zusammenführung und Verarbeitung oben **D.I.2.a.bb.aaa.(1)**). Die Datenanalysen zielen gerade auf die „Gewinnung neuer Erkenntnisse“ (Art. 61a

Abs. 1 Satz 1 BayPAG). Es ist nicht ausgeschlossen, dass Polizeibeamt*innen ihre Sachverhaltsbewertung gerade aus den Ergebnissen der Analyse ableiten und darauf basierend grundrechtsverletzende Maßnahmen anordnen,

> zu dem Gesetzentwurf, der, bis auf kleinste Änderungen, der nun geltenden Regelung entspricht *Petri*, Stellungnahme zum Fragenkatalog im Rahmen der Anhörung des Ausschusses für Kommunale Fragen, Innere Sicherheit und Sport zum Gesetzentwurf zur Änderung des Polizeiaufgabengesetzes und weiterer Rechtsvorschriften am 16. Mai 2024 – **Anlage 11**, S. 18.

Der erheblichen Eingriffsschwere aufgrund der komplexen Methoden kann auch nicht – wie in der Gesetzesbegründung erfolgt – entgegengehalten werden, dass die Software aufgrund ihrer Schnelligkeit und des Nichtauswerfens von „Nichttreffern" der Datensparsamkeit diene. So könne die Analyse den Vorteil bringen, dass Polizeibeamt*innen nur die von der Software für relevant erachteten Daten zur Kenntnis nähmen. Deshalb könne der Softwareeinsatz zum einen weniger eingriffsintensiv sein als eine umfassende manuelle Sichtung. Zum anderen könnten so Zufallstreffer vermieden werden,

> vgl. LT-Drs. 19/1557, S. 25.

Dies vermag die hohe Eingriffstiefe aufgrund der kaum eingeschränkten Möglichkeiten, hochkomplexe Analysemethoden zur Analyse von Daten einzusetzen, die bislang in keinerlei Beziehung stehen und deren Analysewege und Ergebnisse kaum nachvollziehbar verbleiben, nicht aufzuwiegen.

Vor diesem Hintergrund kann gerade nicht angenommen werden, dass

> „[d]urch die weitgehenden Beschränkungen der Methodik […] das spezifische Eingriffsgewicht der neuen Befugnisse des Art. 61a Abs. 1 und 2 näher an einen einfachen Datenabgleich heran[rückt]",
>
> vgl. LT-Drs. 19/1557, S. 29.

Die eingesetzten Methoden unterscheiden sich vielmehr in erheblichem Maße von einem menschlichen analogen Datenabgleich. Sie machen es möglich, binnen weniger Sekunden bislang unverbundene Daten zueinander in Beziehung zu setzen und dadurch aus diesen automatisiert Risiken, Gefahren und Zusammenhänge erstmals zu erkennen und zu bewerten. Sie bringen gerade neue Erkenntnisse für die Gefahrvermeidung und die Verhinderung von Straftaten. Gerade diese Gewinnung neuer, weitreichender Erkenntnisse aus bereits zur Verfügung stehenden Daten begründet das eigenständige Eingriffsgewicht der Maßnahmen,

BVerfGE 165, 363 (396 Rn. 67).

bbb. Keine Vorkehrungen zur Vermeidung von Diskriminierung

Erlaubt die gesetzlich zugelassene Methode eine Auswertung großer Datenmengen insbesondere auch auf statistische Zusammenhänge hin, ist zudem eine ausreichende Datenqualität sicherzustellen und es müssen Vorkehrungen dagegen getroffen sein, dass die Auswahl der einbezogenen Daten unangemessen verzerrende, diskriminierende Wirkungen entfalten kann,

BVerfGE 165, 363 (407 Rn. 95).

Ebenso sind gesetzliche Vorkehrungen erforderlich, wenn im Rahmen von Art. 61a BayPAG Software zur Anwendung kommen kann, die KI oder vergleichbar komplexe deterministische Systeme einsetzt,

BVerfGE 165, 363 (408 Rn. 100).

Schützende Regelungen müssen gesetzlich insbesondere nicht nur für den Einsatz von KI, sondern auch für komplexe deterministische Systeme, deren Software unverändert vorprogrammiert ist, vorgesehen werden, die wegen ihrer Komplexität ebenfalls an Nachvollziehbarkeitsdefiziten leiden. Sie stellen einen hinreichenden Schutz vor der Verwendung diskriminierender Algorithmen sicher,

vgl. BVerfGE 165, 336 (408 f. Rn. 100 f.).

Auch bestehen besondere Risiken, wenn Software privater Akteure oder anderer Staaten eingesetzt wird,

> vgl. BVerfGE 165, 363 (408 Rn. 100).

Auch der EuGH weist darauf hin, dass gerade im Hinblick auf die Gewährleistung von effektivem Rechtsschutz und Kontrolle transparent und nachvollziehbar sein muss, wie eine Software zu dem jeweiligen Ergebnis im Einzelfall kommt,

> vgl. EuGH, Urteil vom 21. Juni 2022, C-817/19, Rn. 195.

Unter Anwendung dieser Grundsätze bedarf es gesetzlicher Vorkehrungen gegen diskriminierende Wirkung der Maßnahmen nach Art. 61a Abs. 1 BayPAG.

Nach Art. 61a BayPAG darf aufgrund der Methodenoffenheit (siehe dazu soeben **D.I.2.a.bb.aaa.**), und mangels expliziten Ausschlusses auch eine Datenauswertung aufgrund statistischer Zusammenhänge erfolgen,

> so auch zu dem Gesetzentwurf, der, bis auf kleinste Änderungen, der nun geltenden Regelung entspricht *Petri*, Stellungnahme zum Fragenkatalog im Rahmen der Anhörung des Ausschusses für Kommunale Fragen, Innere Sicherheit und Sport zum Gesetzentwurf zur Änderung des Polizeiaufgabengesetzes und weiterer Rechtsvorschriften am 16. Mai 2024 – **Anlage 11**, S. 17 f.; *Zöller*, Schriftliche Stellungnahme zum Gesetzentwurf der Staatsregierung für ein Gesetz zur Änderung des Polizeiaufgabengesetzes und weiterer Rechtsvorschriften vom 9. April 2024 (LT-Drs. 19/1557) – **Anlage 12**, S. 15.

Zudem ist der Einsatz von KI zur Vorprogrammierung des Analysesystems nicht hinreichend bestimmt und normenklar ausgeschlossen und Art. 61a BayPAG ermöglicht jedenfalls die Verwendung vergleichbar komplexer deterministischer Systeme (siehe soeben **D.I.2.a.bb.aaa.(2)(c)**).

Dies gilt auch im konkreten Falle, da aufgrund von Art. 61a BayPAG aktuell bereits die Software „VeRA“ des privaten Anbieters Palantir genutzt wird, deren Quellcode und Funktionsweise nicht transparent überprüfbar sind,

zu dem Gesetzentwurf, der, bis auf kleinste Änderungen, der nun geltenden Regelung entspricht *Zöller*, Schriftliche Stellungnahme zum Gesetzentwurf der Staatsregierung für ein Gesetz zur Änderung des Polizeiaufgabengesetzes und weiterer Rechtsvorschriften vom 9. April 2024 (LT-Drs. 19/1557) – **Anlage 12**, S. 16.

Zur Vermeidung von Diskriminierung kommen eine Reihe von technisch-organisatorischen Maßnahmen in Betracht, die zum Teil bereits vor der Anwendungsphase stattfinden. Diese muss der Gesetzgeber zumindest in Grundzügen selbst regeln, die technisch-organisatorische Ausgestaltung kann dann durch die Verwaltung geregelt werden.

Im Bereich der Vorverarbeitung muss die Nutzung ausgewogener Trainingsdaten sichergestellt werden, da die Qualität der softwarebasierten Entscheidung maßgeblich von der Qualität der Trainingsdaten abhängt,

Hüger, Künstliche Intelligenz und Diskriminierung, 2023, S. 158 ff. m.w.N.; *Lauscher/Legner*, ZfDR 2022, 367, (371); *Hacker/Wessel*, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, 53 (53).

Kriterien der Datenqualität sind dabei klassischerweise Richtigkeit, Vollständigkeit, Konsistenz und Aktualität. Im Bereich der künstlichen Intelligenz sind darüber hinaus noch Kriterien wie Ausgewogenheit/Balance und Repräsentativität entscheidend,

Hacker/Wessel, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz/Rostalski (Hrsg.), Künstliche Intelligenz, 2022, 53 (54 f.).

Darüber hinaus ist die Auswahl der Kriterien entscheidend, welche beim maschinellen Lernen genutzt werden. Dies betrifft vor allem den Umgang mit diskriminierend bewerteten Kriterien. Berücksichtigt werden muss jedoch auch, dass einige Merkmale als Stellvertreter („Proxy“) für andere (diskriminierende) Merkmale fungieren können,

Beck, Künstliche Intelligenz und Diskriminierung, 2019, S. 17; *Buchholtz/Scheffel-Kain*, NVwZ 2022, 612 ff.; *Tinhofer*, DRdA 1a/2022,

Heft 399, 170 (172 ff.); *Spiecker/Towfigh*, Automatisch* Benachteiligt Das Allgemeine Gleichbehandlungsgesetz und der Schutz vor Diskriminierung durch algorithmische Entscheidungssysteme, 2023, S. 18.

Dies kann aber nur wirksam umgesetzt werden, wenn der Staat selbst maßgeblichen Einfluss auf die Entwicklung entsprechender Software hat.

Aber auch Maßnahmen zur Transparenzerhöhung kommen in Betracht, wie etwa Tests und Audits, um die Funktionsweise der eingesetzten Software zu rekonstruieren,

Hüger, Künstliche Intelligenz und Diskriminierung, 2023, S. 153 ff. m.w.N.

Unter dem Stichwort „explainability" kommen zudem Maßnahmen in Betracht, die den Algorithmus hinsichtlich der technischen Funktionalität, der logischen Verknüpfung von Eingangs- und Ausgangsdaten und der kausalen Herleitung der Ergebnisse erklärbarer machen,

Tinhofer, DRdA 1a/2022, Heft 399, 170 (176).

Ebenso sind Vorkehrungen zu Vermeidung von automation biases der Polizist*innen bei Nutzung der Analysesysteme erforderlich, da es anderenfalls durch die Überbewertung der Analyseergebnisse zu einer Verstärkung der Diskriminierung kommen kann (siehe dazu **D.I.2.a.bb.aaa.(2)(b)(aa)** am Ende).

Derartige Vorkehrungen sind aber an keiner Stelle vorgesehen.

Insofern die KI-Verordnung der Europäischen Union darauf abzielt, zukünftig Risiken, die mit dem Einsatz von KI verbunden sind, zu identifizieren und diesen entgegenzuwirken, entfaltet diese jedenfalls noch keine Wirkung. Schutzvorkehrungen, die Hoch-Risiko-Systeme betreffen, zu denen „VeRA" gemäß KI-Verordnung Annex III Nr. 6 gehören wird, treten voraussichtlich erst im Juli 2027 in Kraft.

Sofern man den in Art. 61a Abs. 5 Nr. 1 BayPAG enthaltenen Verweis auf Art. 11 JI-Richtlinie auch auf dessen Absatz 2 und Absatz 3 bezieht (dazu

bereits **D.I.2.a.bb.aaa.(2)(b)(bb)**), enthalten auch diese bloße Verbote diskriminierender automatisierter Entscheidungen und Profilings und keine Schutzmaßnahmen, die tatsächlich sicherstellen, dass Diskriminierung unterbleibt.

Auch erforderliche Vorkehrungen zur Entdeckung und Korrektur von Fehlern der eingesetzten Datenauswertungstechnologie,

> BVerfGE 165, 363 (409 Rn. 102),

hat der Gesetzgeber nicht getroffen (siehe hierzu **D.II.2.d.**). Auch im landesrechtlichen Datenschutzrecht finden sich keine ausreichenden Schutzvorkehrungen. Insbesondere im BayDSG, das über Art. 66 BayPAG ergänzende Anwendung findet, sind keine Regelungen zum tatsächlichen Schutz vor Diskriminierungen enthalten. Maßnahmen, die diskriminierende Verarbeitungen und Ergebnisse tatsächlich verhindern sollen, sind gesetzlich nicht vorgesehen.

Auch die defizitär ausgestaltete datenschutzrechtliche Kontrolle vermag keine geeignete Sicherung darzustellen (siehe dazu **D.II.2.**).

b. Art. 61 Abs. 2 Satz 1 Nr. 1 und Nr. 2 BayPAG

Auch bei Art. 61 Abs. 2 Satz 1 Nr. 1 und Nr. 2 BayPAG handelt es sich um schwerwiegende Grundrechtseingriffe. Die für die beiden Tatbestandsvarianten vorgesehenen Einschränkungen hinsichtlich Art und Umfang der verarbeitbaren Daten (**aa.**) reichen im Ergebnis nicht aus, um das Eingriffsgewicht derart signifikant zu reduzieren, dass es sich nur noch um einen weniger gewichtigen Eingriff handelt. Auch die Methode der Datenverarbeitung ist nicht derart eingeschränkt, dass sie zu einer erheblichen Verminderung des Eingriffsgewichts führt (**bb.**).

aa. Keine zureichenden Einschränkungen hinsichtlich Art und Umfang der einbezogenen Daten

Art. 61a Abs. 2 Satz 1 Nr. 1 und Nr. 2 BayPAG sind hinsichtlich Art und Umfang der Daten, die in die Analyse einbezogen werden dürfen, zwar beschränkt. Die Beschränkungen reichen aber nicht aus, um das Eingriffsgewicht signifikant zu reduzieren.

Die für Art. 61a Abs. 2 Satz 1 Nr. 1 und Nr. 2 BayPAG vorgesehenen Beschränkungen in Art. 61a Abs. 3 BayPAG (dazu **aaa.**), Art. 61a Abs. 5 Nr. 3 BayPAG (dazu **bbb.**), Art. 61a Abs. 2 Satz 3 und Satz 4 BayPAG (dazu **ccc.**, **ddd.**) sowie in Art. 61a Abs. 2 Satz 5 BayPAG und Art. 61a Abs. 4 Satz 1 und 2 BayPAG (dazu **eee.**) fallen gering aus. Insbesondere bergen die beiden Tatbestandsvarianten ein hohes Risiko für Unbeteiligte, Ziel polizeilicher Maßnahmen zu werden (dazu **fff.**). Außerdem sind keine organisatorischen oder technischen Vorkehrungen zur Gewährleistung der Zweckbindung getroffen worden (dazu **ggg.**).

aaa. Beschränkung auf bestimmte eigene automatisierte Verfahren (Art. 61a Abs. 3 BayPAG)

Die Beschränkung auf bestimmte, eigene automatisierte Verfahren gemäß Art. 61a Abs. 3 BayPAG bewirkt nur eine geringe Einschränkung hinsichtlich des Umfangs der verarbeitbaren Daten.

Die Tatbestandsvarianten des Art. 61a Abs. 2 Satz 1 BayPAG nehmen Bezug auf Art. 61a Abs. 1 Satz 1 BayPAG, sodass grundsätzlich auf die Ausführungen zu Art. 61a Abs. 1 Satz 1 BayPAG (siehe oben **D.I.2.a.**) verwiesen werden kann, sofern sich keine nur für die Maßnahmen nach Absatz 2 geltenden Besonderheiten ergeben, die im Folgenden näher erörtert werden.

Zunächst enthält Art. 61a Abs. 3 BayPAG spezifische Einschränkungen für Maßnahmen nach Art. 61a Abs. 2 BayPAG: Demnach darf die Polizei nur auf personenbezogene Daten folgender eigener automatisierter Verfahren zugreifen: Vorgangsverwaltungs- und Fallbearbeitungssysteme (Nr. 1), Informations- und Fahndungssysteme (Nr. 2), Kommunikationssysteme (Nr. 3) und Einsatzleit- und Einsatzdokumentationssysteme (Nr. 4).

Von der Beschränkung sind nur die eigenen automatisierten Verfahren erfasst. Demnach bleibt es auch für die Tatbestandsvarianten des Absatzes 2 bei der weitreichenden Erweiterungsmöglichkeit des Art. 61a Abs. 1 Satz 1 Halbsatz 2 BayPAG, die dazu führt, dass eine große Menge weiterer Daten in die Auswertung und Analyse einbezogen und in diesem Rahmen verarbeitet werden können (siehe oben **D.I.2.a.aa.aaa.(3)**). Mithin können Datenquellen (oder jedenfalls mehr oder weniger große Teile davon), die laut der Gesetzesbegründung aufgrund der Einschränkung in Art. 61a Abs. 3 BayPAG von der automatisierten Anbindung ausgeschlossen sein sollen,

> vgl. LT-Drs. 19/1557, S. 28,

dennoch manuell in das System importiert werden, wenn es zu einer konkreten Anwendung kommt. Das betrifft zum Beispiel Systeme zur Verarbeitung von Telekommunikationsverkehrs- und Bestandsdaten. Somit sind insbesondere Verkehrsdaten (siehe dazu oben **D.I.2.a.aa.aaa.(1)**) nicht schlechthin ausgeschlossen. Diese können in großer Menge, gerade wenn sie aus Funkzellenabfragen stammen, im Einzelfall zur Analyse hinzugezogen werden und damit den Umfang der verarbeitbaren Daten erheblich erweitern.

Sofern in der Gesetzesbegründung ausgeführt wird, dass Telekommunikationsverkehrs- und Bestandsdaten erst nach einer erfolgten Relevanzprüfung durch den*die Sachbearbeiter*in einzeln zur weiteren Nutzung manuell hinzuverbunden würden,

> LT-Drs. 19/1557, S. 28,

ist anzumerken, dass diese Beschränkung keinen Anhaltspunkt im Normtext findet und aufgrund der hohen Anforderung an Bestimmtheit und Normenklarheit (siehe oben **D.I.1.b.bb.aaa.**) keine beschränkende Wirkung entfalten kann.

Aber auch die in Absatz 3 gelisteten automatisierten Verfahren stellen keine besonders große Einschränkung hinsichtlich der Menge der verarbeitbaren Daten dar.

Unter Vorgangsverwaltungssystemen versteht der Gesetzgeber EDV-gestützte Anzeigenaufnahme- und Vorgangsverwaltungsprogramme zur Bewältigung des alltäglichen Dienstbetriebes. Damit seien insbesondere alle gemäß Art. 54 Abs. 1 BayPAG gespeicherten Daten, mithin solche zur polizeilichen Aufgabenerfüllung, zur befristeten Dokumentation oder sonstigen Vorgangsverwaltung, erfasst. Die Erfassung der Daten erfolge vorgangsorientiert,

LT-Drs. 19/1557, S. 27.

Die Einbeziehung von Vorgangsverwaltungssystemen stellt sich als besonders eingriffsintensiv dar, da sich diese Systeme durch eine besonders große Menge von Daten mit dem Potenzial, im Umfang erweitert zu werden, sowie dadurch auszeichnen, dass sie eine hohe Zahl personenbezogener Daten unbeteiligter Personen enthält (siehe dazu oben ausführlicher **D.I.2.a.aa.ccc.**).

Bei Fallbearbeitungssystemen handele es sich um Verfahren der bayerischen Kriminalpolizei zur strukturierten Bearbeitung und Analyse von umfangreichen Ermittlungsverfahren sämtlicher kriminalpolizeilicher Phänomenbereiche (z.B. Organisierte Kriminalität (OK), Staatsschutz). Die Erfassung der Daten erfolge hier fallorientiert,

LT-Drs. 19/1557, S. 27.

Informations- und Fahndungssysteme enthalten recherchierbare Daten, insbesondere aus der Personen- und Sachfahndung sowie Auszüge des Kriminalaktennachweises (beschränkt auf das Inhaltsverzeichnis, d.h. ohne Zugriff auf die Kriminalakte selbst), Haftnotierungen, Personenbeschreibungen oder Hinweise und Unterlagen im Zusammenhang mit durchgeführten erkennungsdienstlichen Behandlungen, wie z. B. Lichtbilder,

LT-Drs. 19/1557, S. 28.

Unter Kommunikationssystemen werden unter anderem der dienstliche E-Mailverkehr verstanden,

vgl. LT-Drs. 19/1557, S. 28.

Damit werden grundsätzlich alle E-Mails, die über Arbeitsaccounts verschickt werden, miteinbezogen. Inwiefern bei einer automatisierten Anbindung technisch sichergestellt werden kann, dass Kommunikation, welche nicht dem Zweck der polizeilichen Aufgabenerfüllung diene, nicht eingebunden wird, sondern auf den dienstlichen E-Mail-Verkehr von Funktionspostfächern mit entsprechender Ermittlungsrelevanz beschränkt bleibt, bleibt unklar. Diese vom Gesetzgeber scheinbar intendierte Beschränkung,

so die Gesetzesbegründung, vgl. LT-Drs. 19/1557, S. 28,

spiegelt sich nicht im Gesetzestext wider. Die automatisierte Zusammenführung von jeweils als Einheiten errichteten Systemen legt das Gegenteil nahe. Dass bereits aus Verhältnismäßigkeitsgründen, insbesondere aus der Erforderlichkeit folge, dass nicht alle Daten des Systems zusammengeführt werden, sondern eine Beschränkung auf für die Ermittlungsarbeit relevante Kommunikation erfolge,

vgl. LT-Drs. 19/1557, S. 28,

widerspricht schon dem Sinn und Zweck der Norm. Dies ließe sich nur dadurch umsetzen, dass bei jeder einzelnen E-Mail entschieden würde, ob sie einbezogen wird oder nicht. Dann wäre aber die automatisierte Zusammenführung sinnentleert. Vielmehr ist Absatz 3 so auszulegen, dass der Gesetzgeber für die dort gelisteten Systeme davon ausgeht, dass diese erforderlich sind.

Weiterhin sind Einsatzleit- und Einsatzdokumentationssysteme (Nr. 4) einbezogen. Diese dienen der Dokumentation, Bearbeitung und Steuerung polizeilicher Einsätze für Einsatzleitstellen und Führungsstäbe. Die Daten aus Einsatzleit- und Einsatzdokumentationssystemen dienen insbesondere der Identifikation von polizeilichen Einsätzen, die nicht anderweitig in Vorgangsverwaltungssystemen erfasst wurden und somit für die gefahrenabwehrende Analyse unzugänglich blieben (z.B. polizeiliche Kontrollen oder verdächtige Wahrnehmungen),

LT-Drs. 19/1557, S. 28.

Nach dem Kenntnisstand des Landesdatenschutzbeauftragten werden diese Systeme oftmals auch im Zusammenhang mit Versammlungsgeschehen verwendet,

> zu dem Gesetzentwurf, der, bis auf kleinste Änderungen, der nun geltenden Regelung entspricht *Petri*, Stellungnahme zum Fragenkatalog im Rahmen der Anhörung des Ausschusses für Kommunale Fragen, Innere Sicherheit und Sport zum Gesetzentwurf zur Änderung des Polizeiaufgabengesetzes und weiterer Rechtsvorschriften am 16. Mai 2024 – **Anlage 11**, S. 14

Die Einbeziehung von personenbezogenen Daten, die im Zusammenhang mit der Anmeldung und Durchführung von Versammlungen erhoben wurden, ist bereits vor dem Hintergrund potenziell negativer Auswirkungen, sogenannter Chilling Effects, auf die Versammlungsfreiheit gemäß Art. 8 GG als verfassungsrechtlich bedenklich anzusehen.

Außerdem sind die in Absatz 3 genannten Datentöpfe als Systemtypen und damit auch gewissermaßen abstrakt beschrieben, sodass innerhalb des jeweiligen Systemtypus künftig weitere, noch nach Art. 64 Abs. 1 BayPAG zu errichtende Systeme (siehe dazu auch oben **D.I.2.a.aa.aaa.(1)**) einbezogen werden können.

bbb. Ausschluss des Abgleichs von personenbezogenen Daten aus der Allgemeinheit offenstehenden Netzwerken (Art. 61a Abs. 5 Nr. 3 BayPAG)

Auch für die Tatbestandsvarianten des Art. 61a Abs. 2 Satz 1 Nr. 1 und Nr. 2 BayPAG gilt die Einschränkung des Art. 61a Abs. 5 Nr. 3 BayPAG. Insofern ist auf die Ausführungen im Rahmen der Beurteilung des Eingriffsgewichts des Art. 61a Abs. 1 Satz 1 BayPAG zu verweisen (siehe oben **D.I.2.a.aa.bbb.**).

ccc. Ausschluss von Daten aus verdeckten Zugriffen auf informationstechnische Systeme und dem Einsatz technischer Mittel in Wohnungen (Art. 61a Abs. 2 Satz 3 a.E. BayPAG)

Eine weitere ausschließlich für die Tatbestandsvarianten des Art. 61a Abs. 2 Satz 1 BayPAG geltende Beschränkung findet sich in Art. 61a Abs. 2

Satz 3 a.E. BayPAG. Danach ist die die automatisierte Verarbeitung von personenbezogenen Daten, die durch den Einsatz technischer Mittel in Wohnungen oder durch verdeckten Zugriff auf informationstechnische Systeme erhoben wurden, unzulässig. Damit ist nur ein kleiner Teil von Daten, die aus schwerwiegenden Grundrechtseingriffen stammen,

> vgl. zu dieser Einschränkungsmöglichkeit BVerfGE 165, 363 (402 Rn. 81),

ausgeschlossen.

Neben den Daten aus Telekommunikationsüberwachung (Art. 42 Abs. 1 und 3 bis 4 BayPAG, Art. 43 Abs. 2 BayPAG; § 100a StPO) können auch Daten, die aus dem Einsatz verdeckter Ermittler*innen (Art. 37 BayPAG; § 110a StPO), aus dem Einsatz von Vertrauenspersonen (Art. 38 BayPAG), elektronischer Aufenthaltsüberwachung (Art. 34 Abs. 1 BayPAG), dem Einsatz automatisierter Kennzeichenerkennungssysteme (Art. 39 Abs. 1 BayPAG), Postsicherstellung (Art. 35 Abs. 1 BayPAG), Rasterfahndung (Art. 46 Abs. 1 BayPAG), längerfristiger Observationen (Art. 36 Abs. 1 Nr. 1, Abs. 2 BayPAG; § 163f StPO), oder dem Einsatz technischer Mittel außerhalb von Wohnungen (Art. 36 Abs. 1 Nr. 2, Abs. 2 BayPAG; §§ 100f, 163f StPO) stammen, sowie Nutzungsdaten (Art. 43 Abs. 4 BayPAG; § 100k StPO) einbezogen werden.

ddd. Beschränkung der Datenarten und Datenformate (Art. 61a Abs. 2 Satz 3 und Satz 4 BayPAG)

Art. 61a Abs. 2 Satz 3 und Satz 4 BayPAG schließt zwar bestimmte Datenarten und -formate aus und reduziert damit das Eingriffsgewicht. Diese Reduzierung wirkt sich aber nur gering auf die Bewertung der Eingriffsintensität insgesamt aus.

Art. 61a Abs. 2 Satz 3 BayPAG schließt die automatisierte Verarbeitung von DNA-Erkennungsmustern sowie Finger- und Handflächenabdrücken aus. Art. 61a Abs. 2 Satz 4 BayPAG schließt Video und Audio-Dateien aus.

Zwar kann der Ausschluss biometrischer Daten und eine Regelung zugelassener Datenarten eingriffsmildernd wirken, allerdings kommt es auf die inhaltliche Ausgestaltung an,

BVerfGE 165, 363 (404 Rn. 87).

Gleiches gilt für eine Regelung der einbeziehbaren Dateiformate, wie etwa von Bildern, Video- und Audioaufnahmen in die Datenanalyse oder -auswertung,

BVerfGE 165, 363 (404 Rn. 87).

Diese Beschränkungen sind im Ergebnis als geringfügig zu bewerten.

Zunächst hat der Gesetzgeber sich nicht für eine Positivliste entschieden, wie beispielsweise in § 3 Abs. 1 ATDG. Abgeschlossene Listen mit zugelassenen Datenarten und/oder Datenformaten habe im Vergleich zu partiellen Ausschlüssen eine stärkere beschränkende Wirkung, da sie aufgrund der fehlenden Dynamik ein höheres Maß an Bestimmtheit und Normenklarheit aufweisen.

Darüber hinaus werden nur wenige Datenarten und -formate ausgeschlossen. Gemäß Art. 61a Abs. 2 Satz 3 BayPAG wird nur ein Teil biometrischer Daten ausgeschlossen, nämlich DNA-Erkennungsmuster sowie Finger- und Handflächenabdrücke. Am relevantesten wird mit Blick auf die zu beobachtende Ausweitung polizeilicher Befugnisse, die biometrische Datenabgleiche ermöglichen, aber Bildmaterial sein. Zwar ist die automatisierte Verarbeitung von Audio- und Videomaterial unzulässig, nicht aber von Bildmaterial.

Es ist nicht hinreichend klar, ob sich die Ausschlüsse des Art. 61a Abs. 2 Satz 3 und Satz 4 BayPAG lediglich darauf beziehen, dass die betroffenen Datenarten und -formate von der automatisierten Zusammenführung ausgeschlossen sind (Art. 61a Abs. 1 Satz 1 Halbsatz 1 BayPAG) oder sie auch nicht darauf bezogen verarbeitet werden dürfen, also Teil der Erweiterungsmöglichkeit des Art. 61a Abs. 1 Satz 1 Halbsatz 2 BayPAG sein dürfen. Wenn sie für Art. 61a Abs. 1 Satz 1 Halbsatz 2 BayPAG nicht ausgeschlossen sind, ergibt sich daraus ein besonders hohes Eingriffsgewicht, da dann

Audio- und Videodateien mit den in Art. 61a Abs. 3 BayPAG hinterlegten Bilddateien abgeglichen werden könnten. Jedenfalls aber erfüllt die Einschränkung nicht die Vorgaben an Bestimmtheit und Normenklarheit, die bei heimlichen Maßnahmen besonders hoch sind (siehe oben **D.I.1.b.bb.**).

eee. Anordnungsvorbehalt (Art. 61a Abs. 2 Satz 5 BayPAG) und Zugriffbeschränkung (Art. 61a Abs. 4 Satz 1 und 2 BayPAG)

Zusätzlich zu der Zugriffsbeschränkung in Art. 61a Abs. 4 Satz 1 und 2 BayPAG, die auch für die Tatbestandsvarianten des Art. 61a Abs. 2 Satz. 1 Nr. 1 und Nr. 2 BayPAG gilt (siehe dazu oben ausführlich **D.I.2.a.aa.bbb.**), sieht Art. 61a Abs. 2 Satz 5 BayPAG einen Anordnungsvorbehalt vor, der die Zugriffsbeschränkung verschärft und somit das Eingriffsgewicht geringfügig reduziert. Demnach dürfen Maßnahmen nur durch die in Art. 36 Abs. 4 BayPAG genannten Personen angeordnet werden. Gemäß Art. 36 Abs. 4 Satz 1 BayPAG ist die Anordnung dem*der Leiter*in des Landeskriminalamtes oder eines Präsidiums der Landespolizei vorbehalten. Gemäß Art. 36 Abs. 4 Satz 2 BayPAG kann die Anordnungsbefugnis auf Polizeivollzugsbeamt*innen, die die Ausbildungsqualifizierung für die Ämter ab der vierten Qualifikationsebene absolviert haben, oder Beamt*innen mit der Befähigung zum Richter*innenamt, die in Ämter ab der vierten Qualifikationsebene, fachlicher Schwerpunkt Polizeivollzugsdienst, gewechselt sind, übertragen werden.

Diese zusätzliche Einschränkung kann das Eingriffsgewicht jedenfalls nicht hinreichend reduzieren, sondern dient als verfahrensrechtliche Absicherung, ähnlich wie dies bei schweren Grundrechtseingriffen der Fall ist, die einen Richter*innenvorbehalt voraussetzen. Diese sind gleichwohl als schwerwiegende Eingriffe zu qualifizieren, die nur unter strengen weiteren Voraussetzungen zulässig sind.

fff. Kein Ausschluss der Daten Unbeteiligter

Die für die Tatbestandsvarianten des Art. 61a Abs. 2 Satz 1 BayPAG vorgesehenen Beschränkungen fallen jedoch nur wenig ins Gewicht, weil eine

Vielzahl von personenbezogenen Daten Unbeteiligter in die Analyse einbezogen werden kann. Dieser Aspekt trägt maßgeblich dazu bei, dass sich das Eingriffsgewicht insgesamt als hoch darstellt.

Im Unterschied zu Art. 61a Abs. 1 Satz 1 BayPAG könnte sich allein aus Art. 61a Abs. 3 BayPAG eine mögliche Beschränkung ergeben. Allerdings sind hier explizit Vorgangsverwaltungssysteme benannt, die große Mengen Daten unbeteiligter Personen enthalten (siehe oben **D.I.2.a.aa.ccc.**). Darüber hinaus werden auch in Einsatzleit- und Einsatzdokumentationssystemen Daten vieler Personen gespeichert, die weder einer Straftat oder Ordnungswidrigkeit verdächtig oder von polizeilichen Eingriffsmaßnahmen betroffen, sondern Zeug*innen, Geschädigte, Auskunftspersonen etc. sind,

> zu dem Gesetzentwurf, der, bis auf kleinste Änderungen, der nun geltenden Regelung entspricht *Petri*, Stellungnahme zum Fragenkatalog im Rahmen der Anhörung des Ausschusses für Kommunale Fragen, Innere Sicherheit und Sport zum Gesetzentwurf zur Änderung des Polizeiaufgabengesetzes und weiterer Rechtsvorschriften am 16. Mai 2024 – **Anlage 11**, S. 14.

Auch die anderen in Art. 61a Abs. 3 BayPAG gelisteten Systeme enthalten Daten unbeteiligter Personen.

Da über Art. 61a Abs. 1 Satz 1 Halbsatz 2 BayPAG potenziell weitere Datenbestände manuell importiert und in die Analyse einbezogen werden können (siehe oben **D.I.2.a.aa.aaa.(3)**), können auch weitere Datenbestände, zum Beispiel Verkehrsdaten aus Funkzellenabfragen, die typischerweise eine immense Anzahl an Daten unbeteiligter Personen enthalten, aber auch Telekommunikationsdaten, Extrakte aus Asservaten und Daten aus sozialen Medien, letztere unter dem Vorbehalt des Art. 61a Abs. 5 Nr. 3 BayPAG (siehe dazu ausführlicher oben **D.I.2.a.aa.bbb.** und **D.I.2.a.aa.ccc.**), hinzugezogen werden. Somit besteht für Unbeteiligte ein hohes Risiko, Adressat*innen weiterer Maßnahmen zu werden, was zur Erhöhung des Eingriffsgewichts beiträgt,

> vgl. BVerfGE 165, 363 (400 Rn. 77).

ggg. Keine organisatorischen oder technischen Vorkehrungen zur Gewährleistung der Zweckbindung

Der Umfang der verarbeitbaren Daten ist auch nicht durch organisatorische oder technische Vorkehrungen zur Sicherstellung der Zweckbindung gewährleistet.

Art. 61a Abs. 2 Satz 2 BayPAG stellt zwar klar, dass die Vorschriften des Art. 48 Abs. 1 und 3 PAG, des Art. 53 Abs. 2 PAG sowie des Art. 54 Abs. 2 Satz 1 PAG unberührt bleiben.

Allerdings werden die Grundsätze der Zweckbindung und Zweckänderungen nicht durch organisatorische oder technische Vorkehrungen gesichert, insbesondere ist keine Kennzeichnung der Daten vorgeschrieben (siehe ausführlich oben **D.I.2.a.aa.ddd.**).

bb. Keine zureichende Beschränkung der zugelassenen Methode

Auch hinsichtlich der Datenanalysen gemäß Art. 61a Abs. 2 Satz 1 Nr. 1 und Nr. 2 BayPAG hat der Gesetzgeber keine ausreichenden Einschränkungen der Analysemethode vorgenommen, um das Eingriffsgewicht insgesamt zu reduzieren.

Der Gesetzgeber hat für Art. 61a Abs 2 Satz 1 BayPAG keine weitergehenden Beschränkungen der Analysemethode vorgesehen, als sie für Art. 61a Abs. 1 Satz 1 BayPAG gelten. Diese Beschränkungen reduzieren das Eingriffsgewicht nicht ausreichend (siehe hierzu **D.I.2.a.bb.**). Insbesondere stellen die Ausschlüsse der Art. 61a Abs. 4 Satz 3 sowie Abs. 5 keine ausreichende Beschränkung der Methode sicher (siehe hierzu **D.I.2.a.bb.aaa.(2)**).

Auch im Rahmen von Art. 61a Abs. 2 Satz 1 Nr. 1 und Nr. 2 BayPAG unterscheiden sich die eingesetzten Methoden daher in erheblichem Maße von einem menschlichen analogen Datenabgleich. Sie ermöglichen, binnen weniger Sekunden bislang unverbundene Daten mit komplexen und in ihrer Funktionsweise intransparenten Algorithmen zueinander in Beziehung zu setzen und dadurch aus diesen automatisiert Risiken, Gefahren und Zusammenhänge erstmals zu erkennen und zu bewerten. Sie bringen gerade

neue Erkenntnisse für die Gefahrvermeidung und die Verhinderung von Straftaten.

II. Nichtbeachtung der korrespondierenden Eingriffsvoraussetzungen

Die Tatbestandsalternativen des Art. 61a Abs. 1 und Abs. 2 BayPAG genügen nicht den verfassungsrechtlichen Rechtfertigungsanforderungen, die der Grundsatz der Verhältnismäßigkeit an derart intensive Grundrechtseingriffe stellt (**1.**). Ferner genügt Art. 61a BayPAG insgesamt nicht den verfassungsrechtlichen Anforderungen an Transparenz, individuellen Rechtsschutz und aufsichtliche Kontrolle (**2.**).

1. Eingriffsschwellen und zu schützende Rechtsgüter der Art. 61a Abs. 1 und Abs. 2 Satz 1 Nr. 1 und Nr. 2 BayPAG

Die verfassungsrechtlichen Anforderungen an Eingriffsschwelle und Rechtsgüterschutz ergeben sich daraus, dass es sich bei Art. 61a Abs. 1 Satz 1 ebenso wie – entgegen der gesetzgeberischen Annahme – bei Art. 61a Abs. 2 Satz 1 Nr. 1 und Nr. 2 BayPAG um schwerwiegende Grundrechtseingriffe handelt (dazu **a.**). Es gelten die Maßstäbe zur Rechtfertigung eingriffsintensiver heimlicher Überwachungsmaßnahmen (dazu **a.aa.**).

In Art. 61a Abs. 1 Satz 1 BayPAG ist zwar die zur Rechtfertigung erforderliche Rechtsgüterschwelle vorgesehen. Art. 61a Abs. 1 Satz 1 bleibt jedoch hinter der Eingriffsschwelle zurück, da die Norm auch eine drohende Gefahr zur Rechtfertigung genügen lässt (dazu **a.bb.**).

Auch die in Art. 61a Abs. 2 Satz 1 Nr. 1 und Nr. 2 vorgesehenen Rechtfertigungsvoraussetzungen genügen nicht den verfassungsrechtlichen Anforderungen (dazu **a.cc.**)**.** Art. 61a Abs. 2 Satz 1 Nr. 1 BayPAG sieht keine hinreichenden Eingriffs- und Rechtsgüterschwellen vor und enthält zudem einen unzulässigen dynamischen Verweis auf den bundesrechtlichen § 100b Abs. 2 StPO (dazu **a.cc.aaa.**). Ebenso bleiben die in Art. 61a Abs. 2 Satz 1

Nr. 2 BayPAG zur Rechtfertigung vorgesehen Rechtsgüter und Eingriffsschwellen hinter den verfassungsrechtlichen Anforderungen zurück (dazu **a.cc.bbb.**).

Selbst wenn das Eingriffsgewicht durch Einschränkungen des Gesetzgebers ausreichend reduziert wäre, genügten Art. 61a Abs. 2 Satz 1 Nr. 1 und Nr. 2 BayPAG den verfassungsrechtlichen Anforderungen nicht (dazu **b.**). Dies gilt selbst für den Fall, dass die in Art. 61a Abs. 2 Satz 1 Nr. 2 BayPAG als Eingriffsschwelle vorgesehene drohende Gefahr eine ausreichende Eingriffsschwelle darstellen würde (dazu **c.**).

a. Bei hoher Eingriffsintensität

Da es sich bei Art. 61a Abs. 1 Satz 1 und Abs. 2 Satz 1 Nr. 1 und Nr. 2 BayPAG um schwerwiegende Grundrechtseingriffe handelt, gelten die Maßstäbe zur Rechtfertigung eingriffsintensiver heimlicher Überwachungsmaßnahmen (dazu **aa.**).

aa. Maßstab

Heimliche Überwachungsmaßnahmen und damit auch automatisierte Datenanalysen, die schwerwiegende Grundrechtseingriffe darstellen, sind nur bei einer zumindest hinreichend konkretisierten Gefahr für besonders gewichtige Rechtsgüter zulässig,

> BVerfGE 165, 363 (363 Leitsatz 4, 410 f. Rn. 105 f.).

aaa. Mindestens konkretisierte Gefahr

Für eine automatisierte Datenanalyse, die einen schwerwiegenden Grundrechtseingriff darstellt, muss der Eingriffsanlass streng begrenzt sein. Die verfassungsrechtlich erforderliche Eingriffsschwelle ist hier wie für die meisten heimlichen, tief in die Privatsphäre eingreifenden Überwachungsmaßnahmen der Gefahrenabwehrbehörden die hinreichend konkretisierte Gefahr,

> BVerfGE 165, 363 (410 f. Rn. 106).

Eine hinreichend konkretisierte Gefahr setzt voraus, dass

> „eine Gefährdung dieser Rechtsgüter im Einzelfall hinreichend konkret absehbar ist und der Adressat der Maßnahmen aus Sicht eines verständigen Dritten den objektiven Umständen nach in sie verfangen ist“,
>
> BVerfGE 141, 220 (271 Rn. 109, zu den Rechtsgütern 270 Rn. 108).

Für die Rechtfertigung der automatisierten Datenanalyse als heimliche Ermittlungsmaßnahme mit hohem Eingriffsgewicht bedarf es für die Eingriffsschwelle der konkretisierten Gefahr zweier kumulativer Voraussetzungen, die nur durch eine terrorismusbezogene Ausnahme ersetzt werden können.

Zum einen ist notwendig,

> „dass zumindest tatsächliche Anhaltspunkte für die Entstehung einer konkreten Gefahr für die Schutzgüter bestehen. Allgemeine Erfahrungssätze reichen insoweit allein nicht aus. Vielmehr müssen bestimmte Tatsachen festgestellt sein, die im Einzelfall die Prognose eines Geschehens, das zu einer zurechenbaren Verletzung der hier relevanten Schutzgüter führt, tragen. Eine hinreichend konkretisierte Gefahr in diesem Sinne kann danach schon bestehen, wenn sich der zum Schaden führende Kausalverlauf noch nicht mit hinreichender Wahrscheinlichkeit vorhersehen lässt, sofern bereits bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen. Die Tatsachen müssen dafür […] den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen“,
>
> BVerfGE 165, 363 (410 f. Rn. 106 m.w.N.)

Zum anderen müssen auch tatsächliche Anhaltspunkte bestehen,

> „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“,
>
> BVerfGE 165, 363 (410 f. Rn. 106 m.w.N.).

Um den grundrechtlichen Schutzpflichten des Staates, vor allem auch gegenüber terroristischen Bedrohungen, Rechnung zu tragen, hat das angerufene Gericht im Rahmen der Grundsätze zur konkretisierten Gefahr unter engen Voraussetzungen und ausschließlich im Bereich der terroristischen Straftaten eine personenbezogene statt situationsbezogene Gefährlichkeitsprognose ermöglicht:

> „In Bezug auf terroristische Straftaten, die oft durch lang geplante Taten von bisher nicht straffällig gewordenen Einzelnen an nicht vorhersehbaren Orten und in ganz verschiedener Weise verübt werden, können Überwachungsmaßnahmen auch dann erlaubt werden, wenn zwar noch nicht ein seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennbar ist, jedoch das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie solche Straftaten in überschaubarer Zukunft begehen wird. Denkbar ist das etwa, wenn eine Person aus einem Ausbildungslager für Terroristen im Ausland in die Bundesrepublik Deutschland einreist“,
>
> BVerfGE 141, 220 (272 f. Rn. 112).

Dieser Maßstab gilt eng begrenzt für den Bereich terroristischer Straftaten und kann nicht insgesamt als Eingriffsschwelle für alle zu schützenden Rechtsgüter herangezogen werden,

> BVerfG, Beschluss vom 14. November 2024, 1 BvL 3/22, Rn. 78; BVerfGE 165, 1 (50 Rn. 91).

Werden Daten aus einer Wohnraumüberwachung oder einer Online-Durchsuchung einbezogen, ist dies wegen des besonderen Eingriffsgewichts nur unter den sehr engen Voraussetzungen einer dringenden oder im Einzelfall hinreichend konkretisierten Gefahr zulässig,

> BVerfGE 169, 332 (387 Rn. 136); 165, 363 (402 Rn. 81 m.w.N.).

Darüber hinaus ergeben sich an Bestimmtheit und Normenklarheit der zu regelnden Eingriffsschwellen und zu schützenden Rechtsgüter besondere Anforderungen (siehe hierzu bereits unter **D.I.1.b.bb.**).

bbb. Schutz besonders gewichtiger Rechtsgüter

Heimliche Überwachungsmaßnahmen, die tief in das Privatleben hineinreichen, sind zudem nur zum Schutz besonders gewichtiger Rechtsgüter zulässig, zu denen vor allem Leib, Leben und Freiheit der Person sowie Bestand oder Sicherheit des Bundes oder eines Landes zählen,

> BVerfGE 165, 363 (410 Rn. 105); 141, 220 (270 f. Rn. 108).

Der uneingeschränkte Schutz von Sachwerten ist dem gegenüber gerade nicht ausreichend,

> BVerfGE 141, 220 (270 f. Rn. 108).

Als hinreichend gewichtige Rechtgüter kommen daher nicht schon Sachwerte mit bedeutendem Wert in Betracht, sondern

> „im gesetzlichen Zusammenhang mit der Terrorismusabwehr vielmehr etwa wesentliche Infrastruktureinrichtungen oder sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen […]“,
>
> BVerfGE 141, 220 (287 f. Rn. 155); 165, 363 (410 Rn. 105).

Der Gesetzgeber muss die Rechtsgüter nicht unmittelbar benennen, sondern kann auch an entsprechende Straftaten anknüpfen, deren Verhütung er mit der Befugnis bezweckt,

> BVerfGE 165, 363 (410 Rn. 105 a.E.).

Es genügt dabei nicht ohne weiteres verfassungsrechtlichen Anforderungen, wenn als Eingriffsanlass an Gefährdungstatbestände angeknüpft wird, die tatbestandlich auf Vorbereitungshandlungen im Vorfeld von konkreten Rechtsgutsgefahren oder -verletzungen abstellen,

> BVerfG, Beschluss vom 14. November 2024, 1 BvL 3/22, Rn. 83;
> BVerfGE 165, 363 (438 f. Rn. 170); 141, 220 (273 Rn. 113).

Knüpft der Gesetzgeber an die Begehung solcher Straftaten an, muss er eigens sicherstellen, dass eine bereits konkretisierte oder konkrete Gefahr für das durch den Straftatbestand geschützte Rechtsgut vorliegt,

vgl. BVerfGE 165, 363 (438 f. Rn. 170 m.w.N.); 165, 1 (51 Rn. 92); 163, 43 (94 Rn. 134).

Weder Art. 61a Abs. 1 Satz 1, 2 (dazu **bb.**) noch Art. 61a Abs. 2 Satz 1 Nr. 1 und Nr. 2 BayPAG (dazu **cc.**) genügen diesen Anforderungen.

bb. Art. 61a Abs. 1 Satz 1, 2 BayPAG

Die in Art. 61a Abs. 1 Satz 1 BayPAG vorgesehene Eingriffsschwelle der drohenden Gefahr bleibt hinter der verfassungsrechtlich erforderlichen konkretisierten Gefahr zurück.

aaa. Zu schützende Rechtsgüter und Eingriffsschwelle der konkreten Gefahr

Art. 61a Abs. 1 Satz 1 BayPAG sieht als Anforderungen an die automatisierte Datenanalyse vor, dass diese „zur Abwehr einer Gefahr oder einer drohenden Gefahr für (Nr. 1) Leib, Leben oder Freiheit einer Person, (Nr. 2) den Bestand oder die Sicherheit des Bundes oder eines Landes oder (Nr. 3) Anlagen der kritischen Infrastruktur oder sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen“ erforderlich ist.

bbb. Unzureichende Eingriffsschwelle wegen drohender Gefahr

Die in Art. 61a Abs. 1 Satz 1 BayPAG geregelte Eingriffsschwelle der drohenden Gefahr genügt den Anforderungen an die verfassungsrechtlich gebotene konkretisierte Gefahr nicht,

so auch zu dem Gesetzentwurf, der, bis auf kleinste Änderungen, der nun geltenden Regelung entspricht *Zöller*, Schriftliche Stellungnahme zum Gesetzentwurf der Staatsregierung für ein Gesetz zur Änderung des Polizeiaufgabengesetzes und weiterer Rechtsvorschriften vom 9. April 2024 (LT-Drs. 19/1557) – **Anlage 12**, S. 15; offenlassend *Benamor*, BayVBl 2025, 44 (47) mit Verweis auf laufende verfassungsgerichtliche Verfahren; a.A. *Petri*, Stellungnahme zum Fragenkatalog im Rahmen der Anhörung des Ausschusses für Kommunale Fragen, Innere Sicherheit und Sport zum Gesetzentwurf zur Änderung des Polizeiaufgabengesetzes und weiterer Rechtsvorschriften am 16. Mai 2024 – **Anlage 11**, S. 12 f.

Gemäß Art. 11a Abs. 1 BayPAG liegt eine drohende Gefahr vor,

> „wenn im Einzelfall
>
> 1. das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet oder
>
> 2. Vorbereitungshandlungen für sich oder zusammen mit weiteren bestimmten Tatsachen den Schluss auf ein seiner Art nach konkretisiertes Geschehen zulassen,
>
> wonach in absehbarer Zeit Angriffe von erheblicher Intensität oder Auswirkung zu erwarten sind (drohende Gefahr)".

Diese Eingriffsschwelle bleibt hinter den verfassungsrechtlichen Anforderungen an die konkretisierte Gefahr zurück. Diese gilt unter anderem, weil in die Datenanalyse mangels Einschränkungen der Datenherkunft (siehe hierzu oben **D.I.2.a.aa.aaa.(4)**) auch Daten aus Online-Durchsuchungen einbezogen werden können,

> BVerfGE 165, 363 (402 Rn. 81 m.w.N.).

Es ist dementsprechend auch (bundes-)gesetzgeberische Praxis, streng zwischen konkretisierter und drohender Gefahr im Sinne des Art. 11a Abs. 1 BayPAG zu unterscheiden,

> „Damit unterscheidet sich die konkretisierte Gefahr als Mindestschwelle für Übermittlungen zur Gefahrenabwehr noch einmal deutlich von der weitgehend konturenlosen und in ihren Anwendungsvoraussetzungen weiter abgesenkten, lediglich „drohenden Gefahr", wie sie etwa im Bayerischen Polizeiaufgabengesetz (BayPAG) weitreichend Verwendung findet."
>
> BT-Drs. 20/9345, S. 23.

Erstens fehlt es in Art. 11a Abs. 1 Nr. 1 BayPAG an der verfassungsrechtlich gebotenen Beschränkung der drohenden Gefahr auf terroristische Gefahren (dazu **(1)(a)**). Eine verfassungskonforme Auslegung ist nicht möglich (dazu **(1)(b)**). Zweitens lässt der in Bezug genommene Art. 11a Abs. 1 Nr. 2 BayPAG eine schwächere Prognosegrundlage ausreichen und fordert keine

konkretisierte Gefahr (dazu **(2)**). Drittens führt die Entscheidung des bayerischen Verfassungsgerichtshofs nicht zu einer ausreichenden Eingriffsschwelle des Art. 61a BayPAG (dazu **(3)**).

(1) Unzureichende Begrenzung von Art. 11a Abs. 1 Nr. 1 BayPAG

Art. 11a Abs. 1 Nr. 1 BayPAG genügt den Anforderungen an eine konkretisierte Gefahr nicht.

(a) Unzulässige allgemeine personenbezogene Gefahrenschwelle

Wie bereits näher dargelegt, hat das angerufene Gericht die Möglichkeit einer situationsunabhängigen personenbezogenen konkretisierten Gefahr eng auf die terrorismusbezogene Ausnahme begrenzt, die sich auf die Besonderheiten terroristischer Straftaten stützt (siehe oben **D.II.1.a.aa.aaa.**),

vgl. BVerfGE 141, 220 (272 f. Rn. 112).

Sie lässt sich auf andere Bereiche, etwa auf den Bereich der organisierten Kriminalität, nicht übertragen.

Bei terroristischen Straftaten handelt sich um oft lange geplante Taten von bisher nicht straffällig gewordenen Einzelnen, die an nicht vorhersehbaren Orten und auf ganz unterschiedliche Weisen verübt werden,

BVerfGE 141, 220 (272 f. Rn. 112), BVerfGE 165, 1 (50 Rn. 91).

Terroristische Straftaten zielen gerade auf die plötzliche Verursachung hoher Schäden an gewichtigen Rechtsgütern unter breiter Öffentlichkeitswirkung. Diese Gefährdungslage ist z.B. mit organisierter Kriminalität nicht vergleichbar. Zum einen zielt diese gerade auf die fortgesetzte Begehung von Straftaten ab, sodass eine Anknüpfung an Individualpersonen aufgrund der wiederholten Tätigkeit der Netze nicht erforderlich ist, sondern auf Parallelen in Sachverhalt und Vorgehensweisen abgestellt werden kann. Zum anderen ist organisierte Kriminalität nicht auf eine öffentliche Wirkung in terroristischer Form und nicht von vornherein auf die Verletzung gewichtiger Rechtsgüter ausgerichtet,

Bäcker, Kriminalpräventionsrecht, 2015, S. 118 ff.

Art. 11a Abs. 1 Nr. 1 BayPAG sieht jedoch allgemein und ohne Begrenzung auf die Begehung terroristischer Straftaten als ausreichende Eingriffsschwelle vor, dass das individuelle Verhalten einer Person eine konkrete Wahrscheinlichkeit dafür begründet, dass in absehbarer Zeit Angriffe von erheblicher Intensität oder Auswirkung zu erwarten sind.

Damit überschreitet die drohende Gefahr in Art. 11a Abs. 1 Nr. 1 BayPAG die verfassungsrechtlichen Anforderungen an die konkretisierte Gefahr,

> so auch BayVerfGH, Entscheidung vom 13. März 2025, 5-VIII-18, Vf. 7-VII-18, Vf. 10-VIII-18, Vf. 16-VIII-18, Rn. 186.

(b) Keine Möglichkeit der verfassungskonformen Auslegung

Art. 61a Abs. 1 i.V.m Art. 11a Abs. 1 Nr. 1 BayPAG kann nicht verfassungskonform ausgelegt werden.

Art. 11a Abs. 1 Nr. 1 BayPAG ist aufgrund seiner Systematik und dem ausdrücklichen gesetzgeberischen Willen einer verfassungskonformen Auslegung nicht zugänglich. Selbst wenn Art. 11a Abs. 1 Nr. 1 BayPAG verfassungskonform ausgelegt werden könnte, wäre eine solche Auslegung jedenfalls nicht auf eingriffsintensive Spezialbefugnisse und damit nicht auf Art. 61a Abs. 1 BayPAG übertragbar.

(aa) Keine verfassungskonforme Auslegung von Art. 11a Abs. 1 Nr. 1 BayPAG

Nach der Rechtsprechung des angerufenen Gerichts ist eine Norm nicht für nichtig zu erklären, wenn sie im Einklang mit der Verfassung ausgelegt werden kann,

> siehe etwa BVerfGE 162, 378 (419 ff.); 138, 64 (93 f.); 2, 266 (282).

Eine solche Auslegung muss jedoch nach den allgemeinen Kriterien des Wortlauts, der Systematik, der Entstehungsgeschichte und des Zwecks der Vorschrift möglich sein,

> BVerfGE 138, 64 (94 f.); 122, 39 (60 f.); 119, 47 (274); 88, 145 (166); 69, 1 (55).

Insbesondere darf dem Gesetz kein entgegengesetzter Sinn verliehen, der normative Gehalt der Norm nicht grundlegend neu bestimmt oder das gesetzgeberische Ziel in einem wesentlichen Punkt verfehlt werden. Die Gerichte müssen die gesetzgeberischen Grundentscheidungen respektieren und dürfen sich nicht über den klar erkennbaren Willen des Gesetzgebers hinwegsetzen,

> so BVerfGE 162, 378 (420); 155, 119 (192); 149, 126 (154 f.); 138, 64 (94); 119, 247 (274); 130, 372 (398); 122, 39 (61).

Indizwirkung kommt dabei auch den Gesetzesmaterialien zu,

> BVerfGE 155, 119 (192 f.); 149, 126 (155); 133, 168 (205); 130, 372 (398).

Unter Anwendung dieser Grundsätze ist bereits eine verfassungskonforme Auslegung des Art. 11a Abs. 1 Nr. 1 BayPAG selbst nicht möglich,

> a.A. BayVerfGH, Entscheidung vom 13. März 2025, 5-VIII-18, Vf. 7-VII-18, Vf. 10-VIII-18, Vf. 16-VIII-18, Rn. 187.

Entgegen der Ansicht des bayerischen Verfassungsgerichtshofs,

> BayVerfGH, Entscheidung vom 13. März 2025, 5-VIII-18, Vf. 7-VII-18, Vf. 10-VIII-18, Vf. 16-VIII-18, Rn. 187,

widerspricht eine Auslegung, nach der unter „Angriffen von erheblicher Intensität oder Auswirkung“ für Art. 11a Abs. 1 Nr. 1 BayPAG nur terroristische oder vergleichbare Angriffe zu verstehen seien, diesen Grundsätzen.

Diese Auslegung ist mit Systematik und Entstehungsgeschichte des Art. 11a Abs. 1 BayPAG nicht vereinbar. Die Auslegung des BayVerfGH setzt sich über den klar erkennbaren Willen des Gesetzgebers hinweg.

Systematisch bezieht sich das Tatbestandsmerkmal „Angriffe von erheblicher Intensität oder Auswirkung“ durch seine Stellung im Schlusssatz hinter der Klammer auf Art. 11a Abs. 1 Nr. 1 und Nr. 2 BayPAG. Eine beschränkende Auslegung dieses Merkmals nur für Art. 11a Abs. 1 Nr. 1 BayPAG, aber nicht für Nr. 2, führt zu einer Spaltung eines einheitlich anzuwendenden Merkmals. Aus der Systematik ergibt sich aber eindeutig, dass das

Merkmal bei beiden Nummern den gleichen Regelungsgehalt haben muss. Die differenzierende Auslegung, wie sie der BayVerfGH vertritt, setzt sich über diese Systematik hinweg und zieht das Merkmal entgegen dem Wortlaut in die jeweilige Nummer hinein, um es dort kontextspezifisch auszulegen. Ein anderer denkbarer Anknüpfungspunkt für eine solche Einschränkung ist im Wortlaut von Art. 11a BayPAG nicht ersichtlich.

Darüber hinaus widerspricht eine solche einschränkende Auslegung auch dem historischen Willen des Gesetzgebers. Diesem war ausweislich der Gesetzesbegründung bewusst, dass das angerufene Gericht einen Verzicht auf einen konkretisierten Geschehensablauf „gerade im terroristischen Bereich“ für zulässig erachtet, dies sei aber dem damaligen Streitgegenstand geschuldet. Der Begriff der drohenden Gefahr des BayPAG sei im Hinblick auf das weitere Aufgabenfeld der Polizei gerade nicht auf die Abwehr rein terroristischer Gefahren beschränkt,

> „Diese moderate Arrondierung wird unter dem Begriff einer drohenden Gefahr zwar im PAG umfassender, d.h. auch bei (z.T. weniger eingriffsintensiven) offenen Maßnahmen zur Anwendung gebracht und nicht von vornherein auf die Abwehr rein terroristischer Gefahren beschränkt“,
>
> LT-Drs. 17/16299, S. 9.

Der Gesetzgeber setzt sich mithin bewusst über die engen Grenzen hinweg, die das angerufene Gericht für den Verzicht auf einen konkretisierten Geschehensablauf entschieden hat. Er begründet dies mit dem weiten Aufgabenbereich der Landespolizei und sieht im Tatbestandsmerkmal „Angriffe von erheblicher Intensität und Auswirkung“ – unzutreffend – eine ausreichende Einschränkung,

> „Durch die Beschränkung auf Gefahren durch Gewalttaten von erheblicher Intensität oder Auswirkung für die in Abs. 3 Satz 2 abschließend aufgezählten bedeutenden Rechtsgüter wird einerseits der Grundsatz der Verhältnismäßigkeit besonders beachtet. Andererseits wird dabei zugleich dem, im Verhältnis zum auf die Abwehr terroristischer Straftaten beschränkten präventivpolizeilichen Zu-

> ständigkeitsbereich des BKA, deutlich weitergehenden Zuständigkeitsbereich der Landespolizei Rechnung getragen. Der Landespolizei obliegt die Abwehr eines wesentlich umfänglicheren Bereichs von drohenden Gefahren für bedeutende Rechtsgüter, die jedoch in ihren Wertigkeiten nicht selten einer terroristischen Gefahr gleichkommen und gleichfalls entsprechende Aufklärungs- und ggf. Eingriffsmaßnahmen rechtfertigen, aber eben auch erfordern“,
>
> LT-Drs. 17/16299, S. 10.

Die Ausweitung der Eingriffsschwelle begründet der Gesetzgeber damit, dass im Stadium der drohenden Gefahr eine Zuordnung einer Gefahr in Kategorien wie Terrorismus nicht immer möglich sei, was der Gefahrenabwehr nicht entgegenstehen dürfe,

> LT-Drs. 17/16299, S. 10.

Als vergleichbar gewichtige Gefahren nennt der Gesetzgeber Amokläufe und geplante Mehrfachtötungen, um Eigentum zu erlangen,

> LT-Drs. 17/16299, S. 10.

Auch in der Gesetzesbegründung zur Überführung der Begriffsdefinition aus Art. 11 Abs. 3 in Art. 11a BayPAG heißt es, im Vorfeld einer konkreten Gefahr stehe nicht immer fest, ob sich die Planung auf eine terroristische Straftat beziehe. Das Merkmal der („Gewalttaten von erheblicher Intensität oder Auswirkung“, wie die damalige Entwurfsfassung die Eingriffsschwelle definierte, beschränke den Begriff auf gravierende Gefahrenlagen aufgrund der umfänglicheren Aufgaben der Landespolizei. Auch andere Gefahrenlagen wie Amokläufe dürften nicht aus der drohenden Gefahr ausgeschlossen werden,

> LT-Drs. 18/13716, S. 22.

Der Gesetzgeber hat damit wiederholt seinen Willen zum Ausdruck gebracht, den Verzicht auf ein konkretisiertes erwartbares Geschehen nicht auf die Abwehr terroristischer Straftaten beschränken zu wollen. Die in der Gesetzesbegründung angeführten Beispiele Mord aus Habgier bzw. Raub zeigen, dass die Ausweitung der drohenden Gefahr auch nicht nur für – den

terroristischen Straftaten näherliegende – Amoktaten erfolgen sollte. Vielmehr sollte die „drohende Gefahr“ gemäß Art. 11a BayPAG in beiden Varianten alle Arten von Angriffen auf die dort definierten bedeutenden Rechtsgüter erfassen. Das gilt nach der Gesetzesbegründung ausdrücklich auch für das Tatbestandsmerkmal der „Angriffe von erheblicher Intensität oder Auswirkung“, das der BayVerfGH als Anknüpfungspunkt für die verfassungskonforme Auslegung wählt. Eine Beschränkung des Art. 11a Abs. 1 Nr. 1 BayPAG widerspricht aus diesem Grunde dem deutlich niedergelegten ausdrücklichen Willen des Gesetzgebers.

(bb) Keine verfassungskonforme Auslegung von Art. 61a Abs. 1 i.V.m Art. 11a Abs. 1 Nr. 1 BayPAG

Selbst wenn man eine verfassungskonforme Auslegung von Art. 11a Abs. 1 Nr. 1 BayPAG und eine Beschränkung auf die Abwehr der drohenden Gefahr terroristischer Straftaten als möglich erachtete, wäre eine solche Beschränkung im Wege der verfassungskonformen Auslegung jedoch nicht auf Art. 61a Abs. 1 BayPAG übertragbar,

> a.A. BayVerfGH, Entscheidung vom 13. März 2025, 5-VIII-18, Vf. 7-VII-18, Vf. 10-VIII-18, Vf. 16-VIII-18, Rn. 184 zur Übertragbarkeit auf andere Spezialbefugnisse.

Eine Beschränkung der gesetzlich geregelten Eingriffsschwelle des Art. 61a Abs. 1 Satz 1, 2 i.V.m. Art. 11a Abs. 1 Nr. 1, 2 BayPAG dergestalt, dass eine drohende Gefahr im Sinne des Art. 11a Abs. 1 Nr. 1 BayPAG entgegen dem Wortlaut nur bei der Gefahr terroristischer Straftaten gegeben ist, wäre mit den Grundsätzen der Bestimmtheit und Normenklarheit unvereinbar (siehe dazu oben **D.I.1.b.**). An Befugnisnormen, die zu heimlichen eingriffsintensiven Überwachungsmaßnahmen ermächtigen, sind höhere verfassungsrechtliche Anforderungen an Bestimmtheit und Normenklarheit zu stellen (siehe dazu **D.I.1.b.bb.aaa.**).

Auch die Spezialermächtigung des Art. 61a Abs. 1 BayPAG muss diesen Anforderungen gerecht werden. Dies gilt insbesondere, da es dem Gesetzgeber ohne weiteres möglich gewesen wäre, die erforderliche Beschränkung ausdrücklich in den Gesetzeswortlaut aufzunehmen.

Der bayerische Verfassungsgerichtshof rechtfertigt die Möglichkeit der verfassungskonformen Auslegung der drohenden Gefahr im Rahmen der Generalklausel des Art. 11a Abs. 1 BayPAG damit, dass der Anwendungsbereich der drohenden Gefahr im Rahmen der Generalklausel gering sei und nur in atypischen Ausnahmefällen schwere Grundrechtseingriffe aus Anlass einer drohenden Gefahr erfolgen könnten,

> BayVerfGH, Entscheidung vom 13. März 2025, 5-VIII-18, Vf. 7-VII-18, Vf. 10-VIII-18, Vf. 16-VIII-18, Rn. 190, 194.

Der Verfassungsgerichtshof geht von einer Subsidiarität des Art. 11a BayPAG gegenüber sowohl Art. 11 BayPAG als auch den polizeilichen Spezialbefugnissen aus. Für atypische polizeiliche Maßnahmen, die tief in die Grundrechte eingreifen, bleibe nur ein geringfügiger Anwendungsbereich,

> BayVerfGH, Entscheidung vom 13. März 2025, 5-VIII-18, Vf. 7-VII-18, Vf. 10-VIII-18, Vf. 16-VIII-18, Rn. 116 ff., 190.

Aufgrund des Parlamentsvorbehalts könnten schwerste Grundrechtseingriffe zudem nur ausnahmsweise und nur für eine Übergangszeit auf die Generalklausel gestützt werden. Tiefe Eingriffe in die informationelle Selbstbestimmung seien selbst unter diesen Voraussetzungen nicht zulässig. Maßnahmen, die einem Richtervorbehalt unterliegen oder Dritte betreffen, seien nach Art. 11a BayPAG nicht erlaubt,

> BayVerfGH, Entscheidung vom 13. März 2025, 5-VIII-18, Vf. 7-VII-18, Vf. 10-VIII-18, Vf. 16-VIII-18, Rn. 122 ff., 190, 194.

Art. 11a BayPAG greife zudem nur für „neue, vom Gesetzgeber noch nicht bedachte Gefährdungslagen“,

> BayVerfGH, Entscheidung vom 13. März 2025, 5-VIII-18, Vf. 7-VII-18, Vf. 10-VIII-18, Vf. 16-VIII-18, Rn. 194.

Diese Gesichtspunkte sind auf Art. 61a BayPAG nicht übertragbar. Eine einschränkende Auslegung von Art. 11a Abs. 1 Nr. 1 BayPAG wäre daher jedenfalls nicht auf Art. 61a Abs. 1 Satz 1 BayPAG anwendbar.

Art. 61a Abs. 1 BayPAG ermöglicht schwerwiegende Grundrechtseingriffe (siehe **D.I.2.a.**).

Spezialermächtigungen wie Art. 61a BayPAG dienen gerade dazu, schwere Grundrechtseingriffe auch jenseits atypischer Situationen zu ermöglichen. Bei den automatisierten Datenanalysen in der Ausgestaltung des Art. 61a Abs. 1 und Abs. 2 BayPAG handelt es sich gerade auch um Maßnahmen, die tief in das Recht auf informationelle Selbstbestimmung eingreifen.

Art. 61a BayPAG ist auch nicht subsidiär gegenüber anderen Ermächtigungsgrundlagen, auch soweit Maßnahmen an die drohende Gefahr anknüpfen, da nur die Legaldefinition der drohenden Gefahr in Art. 11a Abs. 1 BayPAG, nicht aber die Subsidiaritätsregelung der Generalklausel in Bezug genommen wird.

Bereits der Gesetzesbegründung zu Art. 61a BayPAG ist zudem zu entnehmen, dass die Norm gerade einer vom Gesetzgeber erkannten Gefährdungslage begegnen, eine noch nicht gesetzlich geregelte Maßnahme zum Umgang mit dieser schaffen und damit den Rahmen für einen regelmäßigen und standardmäßigen Umgang mit der automatisierten Zusammenführung und Analyse von Daten ermöglichen soll,

vgl. LT-Drs. 19/1557, S. 2, 23.

Die Datenanalysen betreffen im Falle der expliziten Anordnung der drohenden Gefahr in Art. 61a BayPAG nicht „neue, vom Gesetzgeber noch nicht bedachte Gefährdungslagen“.

Bei der automatisierten Datenanalyse nach Art. 61a Abs. 1 BayPAG handelt es sich zudem gerade um eine heimliche Maßnahme mit erheblicher Eingriffswirkung, die ohne Wissen der Bürger*innen erfolgt und weitere heimliche Ermittlungsmaßnahmen nach sich ziehen kann.

Aus diesen Gründen können die vom bayerischen Verfassungsgerichtshof entwickelten Einschränkungen nicht auf Art. 61a Abs. 1 BayPAG übertragen werden.

Das angerufene Gericht hat zudem mit Blick auf die höheren Anforderungen an Bestimmtheit und Normenklarheit bei Ermächtigungsgrundlagen

zu schwerwiegenden Grundrechtseingriffen wie heimlichen Datenverarbeitungen mehrmals eine verfassungskonforme Auslegung sicherheitsrechtlicher Spezialermächtigungen abgelehnt.

So hat das Gericht eine verfassungskonforme Auslegung des § 45 Abs. 1 Satz 1 Nr. 4 BKAG unter anderem deshalb abgelehnt, weil die Norm heimliche Datenerhebungen ermögliche, die tief in die Privatsphäre eingreifen könnten und deshalb strenge Anforderungen an die Bestimmtheit und Normenklarheit zu stellen seien,

> BVerfGE 169, 332 (371 ff. Rn. 95, 96 ff., 113 ff.).

Auch eine verfassungskonforme Auslegung des § 16a Abs. 1 Satz 1 Nr. 2 i.V.m. § 17 Abs. 1 Satz 1 Nr. 2 des Polizeigesetzes Nordrhein-Westfalen hat das angerufene Gericht mit dem Argument abgelehnt, dass die längerfristige Observation unter gleichzeitiger Anfertigung von Lichtbildern ein hohes Eingriffsgewicht aufweise und deshalb strenge Anforderungen an die Bestimmtheit zu stellen seien,

> BVerfG, Beschluss vom 14. November 2024, 1 BvL 3/22, Rn. 106.

Zu keinem anderen Ergebnis führt, dass das angerufene Gericht eine verfassungskonforme Auslegung des § 20k Abs. 1 Satz 2 BKAG a.F. für zulässig erachtet hat,

> BVerfGE 141, 220 (305, 213 f.); vgl. den Verweis des BayVerfGH, Entscheidung vom 13. März 2025, 5-VIII-18, Vf. 7-VII-18, Vf. 10-VIII-18, Vf. 16-VIII-18, Rn. 187.

Die Entscheidung ist nicht auf die vorliegende Konstellation des Art. 61a BayPAG übertragbar. Nach § 20k Abs. 1 Satz 2 BKAG a.F. durfte das BKA eine Online-Durchsuchung zur Abwehr von Gefahren des internationalen Terrorismus vornehmen, wenn bestimmte Tatsachen auf eine im Einzelfall durch bestimmte Personen drohende Gefahr für eines der in Satz 1 genannten Rechtsgüter hinwiesen. Das angerufene Gericht hat die Norm verfassungskonform dahingehend ausgelegt, dass die beiden Komponenten der konkretisierten Gefahr (wenigstens der Art nach konkretisiertes, zeitlich absehbares Geschehen und Erkennbarkeit der Beteiligung bestimmter

Personen) oder alternativ die konkrete Wahrscheinlichkeit einer Straftatbegehung aufgrund des individuellen Verhaltens einer Person vorliegen mussten,

BVerfGE 141, 220 (305 Rn. 213 f.).

Es definiert den Begriff der „drohenden Gefahr“ damit unter Rückgriff auf seine frühere Rechtsprechung. Hierfür ergaben sich aufgrund der klassischen Auslegungsmethoden aber hinreichende Anhaltspunkte. § 20k Abs. 1 Satz 2 BKAG a.F. verwendete ausdrücklich den Begriff der „drohenden Gefahr“, ohne dass eine gesetzliche Definition vorgesehen war. Die Formulierung der Norm entsprach nahezu wortgenau der Formulierung in BVerfGE 120, 274 (329), sodass anzunehmen war, dass der Gesetzgeber sich auf die ebenfalls dort genannte Definition bezog,

so auch BVerfGE 141, 220 (305 Rn. 214).

Derartige Anhaltspunkte fehlen bei Art. 61a BayPAG. Der dort verwendete Begriff der „drohenden Gefahr“ wird in Art. 11a BayPAG legaldefiniert, sodass ein unmittelbarer Rückgriff auf die Rechtsprechung des angerufenen Gerichts ausscheidet. In Art. 11a Abs. 1 Nr. 1 BayPAG ist die notwendige Beschränkung auf terroristische Angriffe nicht enthalten. Wie gesehen, ist sie auch mit der systematischen Auslegung der Norm nicht vereinbar. Schließlich ergibt sich aus der Gesetzesbegründung eindeutig, dass der Gesetzgeber die vom angerufenen Gericht geforderte Beschränkung auf terroristische Angriffe gerade nicht übernehmen, sondern die Legaldefinition auch auf andere drohende Straftaten wie Mord aus Habgier und Raub erstrecken wollte (siehe jeweils oben unter **D.II.1.a.bb.bbb.(1)(b)(aa)**).

Daher bleibt auch ohne Auswirkung, dass der Gesetzgeber bei Erlass des Art. 61a BayPAG von einer Übereinstimmung von konkretisierter und drohender Gefahr ausging,

vgl. LT-Drs. 19/1557, S. 26.

Auch bei verfassungskonformer Beschränkung des Begriffs der „drohenden Gefahr“ gemäß Art. 11a Abs. 1 Nr. 1 BayPAG auf terroristische und vergleichbare Angriffe verstößt Art. 61a Abs. 1 Satz 1, 2 BayPAG daher gegen

den Grundsatz der Bestimmtheit und Normenklarheit. Bereits für die normanwendende Verwaltung wäre durch den Verweis auf den Begriff der drohenden Gefahr in Art. 11a Abs. 1 BayPAG nicht ausreichend eingegrenzt, dass eine automatisierte Datenanalyse aus Anlass einer drohenden Gefahr wegen des individuellen Verhaltens (Art. 11a Abs. 1 Nr. 1 BayPAG) nur wegen terroristischer Straftaten zulässig wäre, obwohl hierzu keine Anhaltspunkte im Gesetz erkennbar sind.

Jedenfalls für Bürger*innen wäre eine solche einschränkende Auslegung im Rahmen der Verweisung nicht mehr nachvollziehbar, sodass eine Ausrichtung des individuellen Verhaltens anhand des Art. 61a Abs. 1 Satz 1 BayPAG nicht möglich wäre.

Das Rechtsstaatsprinzip gebietet, dass der Gesetzgeber eine eigene Entscheidung im Rahmen des verfassungsrechtlich Möglichen trifft und eine eigene Grundrechtsabwägung zum Ausgleich der widerstreitenden Interessen vornimmt. Entscheidet sich der Gesetzgeber wie vorliegend erkennbar für eine verfassungswidrige Einschränkung der Grundrechte, ist es notwendig, dass er selbst eine neue grundrechtskonforme Abwägung trifft. Die zu weite und unbestimmte Fassung des Art. 61a Abs. 1 i.V.m Art. 11 Abs. 1 Nr. 1 BayPAG würde durch eine verfassungskonforme Auslegung trotz entgegenstehender Systematik und ausdrücklich entgegenstehendem Willen des Gesetzgebers auf das zulässige Maß begrenzt. So würden heimliche Datenanalysen auch gegen Dritte und bislang Unbeteiligte ermöglicht, ohne dass es zu einer gesetzgeberischen Diskussion von Alternativen käme. Vor diesem Hintergrund wird eine verfassungskonforme Auslegung hier den Grundrechten der Betroffenen nicht gerecht. Es bedarf einer Nichtigerklärung des Art. 61a Abs. 1 Satz 1 BayPAG.

(2) Fehlende Begrenzung des Art. 11a Abs. 1 Nr. 2 BayPAG

Art. 11a Abs. 1 Nr. 2 BayPAG bleibt hinter den Anforderungen der konkretisierten Gefahr zurück, da er keine ausreichende tatsächliche und personenbezogene Konkretisierung fordert.

(a) Unzureichende personelle Konkretisierung der Gefahr

Für eine konkretisierte Gefahr bedarf es beider Voraussetzungen, also bestimmter Tatsachen, die den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen und (zugleich) auch den Schluss darauf zulassen, 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,

BVerfGE 165, 363 (410 f. Rn. 106 m.w.N.).

Es ist gerade nicht ausreichend, wenn nur die erste der beiden Voraussetzungen als Eingriffsschwelle genügt und auf den Personenbezug der konkretisierten Gefahr ersatzlos (und ohne Bezug auf die enge terrorismusbezogene Ausnahme) verzichtet wird.

Art. 11a Abs. 1 Nr. 2 BayPAG lässt jedoch gerade Vorbereitungshandlungen, die „für sich oder zusammen mit weiteren bestimmten Tatsachen den Schluss auf ein seiner Art nach konkretisiertes Geschehen zulassen“, genügen, ohne gleichzeitig auch zu verlangen, dass aufgrund der Prognose Personen beteiligt sein werden, über deren Identität bereits zumindest so viel bekannt ist, dass die Überwachungsmaßnahme gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden kann.

Dass „Vorbereitungshandlungen“ gefordert werden, stellt allein keine ausreichende adressat*innenbezogene Begrenzung her, da ein weitergehender Zusammenhang zu bestimmten Personen nicht verlangt wird. Es könnten vielmehr auch allgemeine Informationen über Vorbereitungshandlungen zum Anlass für Datenanalysen genommen werden, beispielsweise Informationen über eine Lieferung von gefährlichen Chemikalien, Waffen oder explosiven Stoffen an einen eingegrenzten Ort, um ohne jegliche personelle Eingrenzung Datenanalysen gegen Personen vorzunehmen, nur weil sie einem bestimmten Profil entsprechen oder beispielsweise in räumlicher Nähe aufhältig waren oder wohnhaft sind.

Die gesetzliche Anknüpfung an die auf bestimmte Tatsachen gestützte Annahme, dass Personen Straftaten vorbereiten, ist selbst dann nicht als Eingriffsschwelle ausreichend, wenn sich die Vorbereitungshandlungen auf terroristische Straftaten beziehen und keine weiteren Eingriffsschwellen vorausgesetzt werden,

> BVerfGE 141, 220 (310 Rn. 232).

Im Erst-recht-Schluss kann daher das bloße Anknüpfen an Vorbereitungshandlungen, die den Schluss auf ein seiner Art nach konkretisiertes Geschehen zulassen, nicht genügen.

(b) Keine personelle Konkretisierung durch andere Rechtsvorschriften

Die erforderliche personelle Konkretisierung der Gefahr kann vorliegend auch nicht aus Art. 61a Abs. 1 BayPAG selbst gefolgert werden. Art. 61a BayPAG sieht selbst keine personellen Einschränkungen bzw. spezielle Adressat*innenregelungen vor. Die Norm enthält über die Begriffe der Gefahr und der drohenden Gefahr hinaus keine speziellen Vorgaben, gegen wen eine Datenanalyse nach Art. 61a Abs. 1 BayPAG eingesetzt werden darf.

Ebenso wenig ist ein Rückgriff auf die Regelungen der Art. 7 ff. BayPAG möglich. Die Grundsätze der Maßnahmerichtung finden auf die drohende Gefahr, jedenfalls jedoch in Art. 61a Abs. 1 BayPAG keine Anwendung.

Die Art. 7 ff. BayPAG, die die Richtung von Maßnahmen an Störer*innen regeln, sind schon deshalb auf die drohende Gefahr nicht anwendbar, da sie stets eine „Gefahr“ voraussetzen (Art. 7 Abs. 1, 3, Art. 8 Abs. 1, 3, Art. 10 Abs. 1 Nr. 1 BayPAG), womit nach der Legaldefinition des Art. 11 Abs. 1 Satz 2 BayPAG ausschließlich eine „konkrete Gefahr“ und nicht eine „drohende Gefahr“ im Sinne des Art. 11a BayPAG gemeint ist,

> so auch BayVerfGH, Entscheidung vom 13. März 2025 - 5-VIII-18, Vf. 7-VII-18, Vf. 10-VIII-18, Vf. 16-VIII-18, Rn. 125.

Ob eine analoge Anwendung der Art. 7 ff. BayPAG für Maßnahmen nach Art. 11a BayPAG selbst in Betracht kommt,

so BayVerfGH, Entscheidung vom 13. März 2025 - 5-VIII-18, Vf. 7-VII-18, Vf. 10-VIII-18, Vf. 16-VIII-18, Rn. 125,

ist dabei im vorliegenden Fall nicht entscheidend.

Damit die allgemeinen Grundsätze der Störer*innenverantwortlichkeit auf die drohende Gefahr in der konkret gegenständlichen Norm des Art. 61a Abs. 1 BayPAG analog angewendet werden können, müssen gerade bezüglich dieser Norm die Analogievoraussetzungen gegeben sein.

Dabei fehlt es bereits an einer planwidrigen Regelungslücke.

Art. 61a BayPAG regelt die Voraussetzungen für die automatisierte Zusammenführung und Verarbeitung von Daten abschließend. In der Gesetzesbegründung sind über die gesetzlich geregelten Anforderungen hinaus keine Einschränkungen des Adressat*innenkreises ersichtlich. Bei Art. 61a BayPAG handelt es sich um eine besondere Rechtsgrundlage für eine spezifische Eingriffsmaßnahme, für die der Gesetzgeber die Voraussetzungen nicht unter Rückgriff auf die Art. 7 ff. BayPAG regeln wollte.

Im Bewusstsein der hohen Anforderungen an Bestimmtheit und Normenklarheit für Rechtsgrundlagen zur Datenanalyse und -auswertung hat der Gesetzgeber andere allgemeine Normen des BayPAG, insbesondere zu den Zweckbindungsgrundsätzen in Art. 61a Abs. 1 Satz 3 BayPAG, explizit in Bezug genommen,

LT-Drs. 19/1557, S. 25 mit Verweis auf BVerfGE 165, 363 (415 Rn. 114).

Eine solch klarstellende Regelung ist in Bezug auf die Art. 7 ff. BayPAG gerade nicht erfolgt.

Eine Störerrichtung der Maßnahme ist gesetzgeberisch gerade nicht gewollt. Der Einsatz soll vielmehr personenoffen mit beliebigen Suchbegriffen möglich sein und so die Auswertung der gesamten einbezogenen Datensätze ermöglichen. Die Analyse ist bewusst nicht begrenzt auf Personen im Sinne der Art. 7 ff. BayPAG, da auch bislang nicht erkannte Verbindungen von Personen oder Informationen sichtbar gemacht werden sollen.

Dies ergibt sich schon aus der systematischen Stellung des Art. 61a BayPAG. Die Ermächtigungsgrundlage für die automatisierte Zusammenführung und Verarbeitung von Daten steht im III. Abschnitt des BayPAG zur Datenverarbeitung und nicht wie andere spezielle Ermächtigungsgrundlagen im II. Abschnitt „Befugnisse der Polizei“, in dem die übrigen Maßnahmen i.S.d. Art. 7 Abs. 1, Art. 8 Abs. 1 BayPAG geregelt sind.

Jedenfalls liegt keine vergleichbare Interessenlage vor.

Für die Einschränkung der Eingriffsschwelle bei der automatisierten Datenanalyse sind die allgemeinen Störer*innengrundsätze nicht geeignet. Diese knüpfen gerade an die tatsächlichen Sachverhaltspunkte einer konkreten Gefahr an. Im Rahmen der drohenden Gefahr will der Gesetzgeber die Datenanalyse aber eben im Vorfeld solcher konkreter (und aufgrund des Wortlauts des Art. 11a Abs. 1 BayPAG auch unzulässigerweise im Vorfeld von konkretisierten) Gefahren ermöglichen.

Ziel der Maßnahme ist es, dass bei den vorgesehenen konkreten oder drohenden Gefahren für die in Art. 61a Abs. 1 Satz 1 Nr. 1-3 BayPAG genannten Rechtsgüter relevante Informationen durch Suchbegriffe in allen vorhandenen Polizeidatensätzen ausgewertet werden können, um so auch neue Beziehungen zu entdecken. Die automatisierte Datenanalyse dient gerade zur

> „automatisierten Zusammenführung zur konkreten Gefahrenabwehr erforderlicher, jedoch bislang unverbundener Dateien und Datenquellen […]“,
>
> LT-Drs. 19/1557, S. 23.

Dabei sollen über bislang bekannte Störer*innen gerade auch durch Daten anderer Personen Verbindungen hergestellt werden können.

Zudem bliebe auch eine Anwendung der Art. 7 ff. BayPAG hinter den verfassungsrechtlichen Anforderungen an eine personelle Konkretisierung der (konkretisierten) Gefahr zurück:

Erstens wären bei einer analogen Anwendung der Vorschriften zur Maßnahmerichtung dann auch automatisierte Datenanalysen gegenüber bloßen Zustandsstörer*innen nach Art. 8 Abs. 1, 2, 3 BayPAG möglich. Gäbe es beispielsweise Anhaltspunkte für die mögliche Gefährdung einer oder mehrerer Gemeinschaftsunterkünfte, z.B. von Geflüchtetenunterkünften, wären Datenanalysen sowohl gegen alle Bewohner*innen der Unterkünfte als auch gegen deren Eigentümer*innen und Leitungspersonal denkbar. Eine Ausübung tatsächlicher Gewalt über die Quelle einer drohenden (also gerade noch nicht konkreten und damit letztlich zukünftigen) Gefahr oder Eigentum an einer solchen genügt gerade nicht als Anhaltspunkt für eine Beteiligung einer bestimmten Person. Genau dies ist jedoch für eine konkretisierte Gefahr in personeller Sicht erforderlich. Tatsächliche oder dingliche Positionen zu Sachen allein können keine grundrechtsinvasiven Datenanalysen rechtfertigen.

Zweitens kämen bei einer Übertragung der Grundsätze zur Maßnahmerichtung gerade auch Datenanalysen gegenüber Nichtstörer*innen gemäß Art. 10 BayPAG in Betracht, wenn Analysen gegen Handlungs- und Zustandsstörer*innen nicht möglich wären oder keinen Erfolg versprächen. Maßnahmen nach Art. 61a Abs. 1 Satz 1 BayPAG gegen gänzlich Unbeteiligte sind – auch unter den Voraussetzungen des Art. 10 Abs. 1 BayPAG – verfassungsrechtlich nicht zu rechtfertigen.

Eine Ergänzung der Eingriffsschwelle des Art. 61a Abs. 1 Satz 1 i.V.m. Art. 11a Abs. 1 Nr. 2 BayPAG um die Grundsätze der Störer*innenverantwortung genügt jedenfalls den Anforderungen an Bestimmtheit und Normenklarheit nicht (siehe zum Maßstab **D.I.1.b.bb.**).

Für normanwendende Polizist*innen wären trotz fehlender weiterer Einschränkungen des Art. 11a Abs. 1 Nr. 2 BayPAG nur in dieser Variante der Eingriffsschwelle für Art. 61a Abs. 1 Satz 1 BayPAG punktuell die Störer*innengrundsätze heranzuziehen. Bei der Anknüpfung an Vorbereitungshandlungen müssten sodann zur Maßnahmerichtung Störer*innen ermittelt werden, die in allen anderen Varianten der Eingriffsschwellen

des Art. 61a BayPAG keine Rolle spielen. Dieses Vorgehen führt schon aufgrund der unterschiedlichen personellen Maßstäbe zwischen Art. 11a Abs. 1 Nr. 1 und Nr. 2 BayPAG in der Eingriffsschwelle zu Anwendungsproblemen. Zudem ist die Bestimmung von Verhaltens- und Zustandsstörer*innen ohne konkrete Gefahr als Anhaltspunkt deutlich schwieriger möglich.

Selbst wenn man in dieser Anwendbarkeit von einer ausreichenden Bestimmtheit der Norm für die normanwendende Verwaltung ausgehen würde, genügte die Heranziehung der Art. 7 ff. in Art. 11 Abs. 1 Nr. 2 BayPAG in Art. 61a Abs. 1 Satz 1 BayPAG nicht den erhöhten Anforderungen an die Normenklarheit an Ermächtigungsgrundlagen zu tiefgreifenden heimlichen Überwachungsmaßnahmen. Die nicht im Wortlaut erkennbare Einschränkung auf die Art. 7 ff. BayPAG innerhalb einer bereits erfolgten Verweisung ist für Bürger*innen nicht mehr nachvollziehbar.

Hätte der Gesetzgeber eine Beschränkung der drohenden Gefahr aus Art. 11a Abs. 1 Nr. 2 BayPAG in personeller Hinsicht vornehmen wollen, wäre es notwendig gewesen, dies im Wortlaut der Norm niederzulegen. Auch hier darf eine verfassungskonforme Auslegung nicht zulasten der Bestimmtheit und Normenklarheit und damit zulasten der Transparenz und des Grundrechtsschutzes der Bürger*innen korrigieren, dass der Gesetzgeber seinen Pflichten zur Regelung angemessener Eingriffsschwellen wissentlich nicht nachgekommen ist.

(3) Keine Verfassungskonformität durch landesverfassungsgerichtliche Entscheidung

Auch die Entscheidung des bayerischen Verfassungsgerichtshofs selbst führt nicht zu einer ausreichenden Eingriffsschwelle im Rahmen von Art. 61a BayPAG.

Zwar hat der Verfassungsgerichtshof in seiner Entscheidung zu Art. 11a BayPAG eine verfassungskonforme Auslegung im Wege einer Beschränkung des Art. 11a Abs. 1 Nr. 1 BayPAG auf die Gefahr terroristische Strafta-

ten sowie eine Übertragung der Art. 7 ff. BayPAG zur personellen Konkretisierung des Art. 11a Abs. 1 Nr. 2 BayPAG vorgenommen (siehe hierzu ausführlich **D.II.1.a.bb.bbb.(1)** und **(2)**),

> BayVerfGH, Entscheidung vom 13. März 2025, 5-VIII-18, Vf. 7-VII-18, Vf. 10-VIII-18, Vf. 16-VIII-18, Rn. 125, 184, 187.

Diese Entscheidung führt jedoch nicht dazu, dass für die in Art. 61a BayPAG genannte drohende Gefahr von einer verfassungskonformen Eingriffsschwelle ausgegangen werden kann.

Den Entscheidungen des bayerischen Verfassungsgerichtshofs kommt, anders als denen des Bundesverfassungsgerichts (§ 31 Abs. 2 BVerfGG), keine Gesetzeskraft zu. Sie sind lediglich im Gesetz- und Verordnungsblatt zu veröffentlichen, wenn eine Rechtsvorschrift – wie hier – nur in einer bestimmten Auslegung für verfassungsgemäß erklärt wird, Art. 25 Abs. 7 Gesetz über den bayerischen Verfassungsgerichtshof (BayVerfGHG), und für andere bayerische Verfassungsorgane, Gerichte und Behörden bindend, Art 29 Abs. 1 BayVerfGHG. Eine Veröffentlichung der Entscheidungsformel und Leitsätze ist erfolgt,

> Bayerisches Gesetz- und Verordnungsblatt (BayGVBl.) 2025, Nr. 7, München, den 15. April 2025, S. 90 ff.

Daraus ergibt sich keine Verfassungskonformität der drohenden Gefahr im Rahmen von Art. 61a Abs. 1 Satz 1 BayPAG. Allein eine behördliche Bindung an eine Gerichtsentscheidung kann für schwerwiegende Grundrechtseingriffe nicht in gleichem Maße verfassungskonformes Handeln sicherstellen. Dies gilt umso mehr wegen der hohen Anforderungen der gesetzlichen Regelungen, die sich aus der Wesentlichkeitstheorie ergeben (siehe dazu bereits **D.I.1.b.aa.**)

Jedenfalls stellt die Entscheidung und die Bindung der bayerischen Verwaltung an diese aber keine verfassungskonforme Rechtslage im Rahmen des Art. 61a BayPAG her, da der Verfassungsgerichtshof nur zu Art. 11a BayPAG selbst als Eingriffsgrundlage entschieden hat. Die Grundsätze sind wie bereits dargestellt (siehe dazu **D.II.1.a.bb.bbb.(1)(b)(bb)**) nicht auf

eine Rechtsgrundlage für eine automatisierte Datenanalyse übertragbar. Jedenfalls bezieht die Entscheidung Art. 61a BayPAG nicht einmal im enthaltenen Obiter Dictum zur Übertragung der Rechtsprechung auf Spezialbefugnisse ein, da Art. 61a BayPAG nicht Verfahrensgegenstand war und in der Entscheidung nicht genannt ist,

> BayVerfGH, Entscheidung vom 13. März 2025, 5-VIII-18, Vf. 7-VII-18, Vf. 10-VIII-18, Vf. 16-VIII-18, Rn. 184.

Selbst wenn man eine solche Bindung an die Entscheidung auch im Rahmen von Art. 61a BayPAG annähme, wäre diese für normanwendende Polizist*innen und Gerichte, vor allem aber Bürger*innen nicht mehr nachvollziehbar, sodass jedenfalls insoweit von mangelnder Bestimmtheit und Normenklarheit auszugehen ist.

Der Gesetzgeber hat die Einschränkungen zur drohenden Gefahr gerade nicht wie erforderlich im Rahmen von Art. 61a BayPAG normiert. Dies kann nicht durch eine landesverfassungsgerichtliche Entscheidung zu einer Generalklausel korrigiert werden, die sich nicht auf die hier gegenständliche Ermächtigungsgrundlage für schwerwiegende Grundrechtseingriffe bezieht.

Anderenfalls müsste das Bundesverfassungsgericht bei vorangehenden Entscheidungen eines Landesverfassungsgerichts stets dessen Auslegungen für seine eigene Entscheidung über die Verfassungsgemäßheit einer Norm zugrunde legen und könnte nicht selbst zum Ergebnis kommen, eine verfassungskonforme Auslegung der Norm sei nicht mehr möglich. Zwischen landesverfassungsrechtlichen und bundesverfassungsgerichtlichen Verfahren besteht jedoch weder ein zeitlicher Vorrang noch eine Subsidiarität, die Verfassungsgerichte stehen selbstständig nebeneinander,

> vgl. BVerfGE 6, 376 (382); *Bethge* in: Schmidt-Bleibtreu/Klein/Bethge, 64. EL August 2024, Teil B Vorb., Rn. 279.

Selbst bei einer Bindungswirkung der Entscheidung sind wie bereits dargestellt (**D.II.1.a.bb.bbb.(1)(b)(bb)**) die vom Verfassungsgerichtshof in Ziffer 2 der Entscheidungsformel definierten Grenzen der Anwendbarkeit

der drohenden Gefahr auf alle Eingriffsermächtigungen mit präventiver Zielrichtung vorliegend nicht eingehalten. Art. 61a BayPAG ermöglich zum einen schwerste Grundrechtseingriffe nicht nur für eine Übergangszeit und aufgrund einer vom Gesetzgeber erkannten Gefährdungslage, der er spezifisch mit Art. 61a BayPAG als Ermächtigungsgrundlage zur Datenanalyse begegnet. Zum anderen greifen Maßnahmen nach Art. 61a BayPAG gerade auch tief in das Recht auf informationelle Selbstbestimmung ein. Auch bei Anwendung der Maßstäbe des bayerischen Verfassungsgerichtshofs stellt die drohende Gefahr keine taugliche Eingriffsschwelle für grundrechtsintensive automatisierte Datenanalysen dar.

cc. Art. 61 Abs. 2 BayPAG

Da auch im Falle von Art. 61a Abs. 2 Satz 1 Nr. 1 und Nr. 2 BayPAG ein schwerwiegender Grundrechtseingriff anzunehmen ist, genügen die geregelten Eingriffsschwellen nicht zur Rechtfertigung der mit den Datenanalysen einhergehenden Grundrechtseingriffe,

> so auch zu dem Gesetzentwurf, der, bis auf kleinste Änderungen, der nun geltenden Regelung entspricht *Petri*, Stellungnahme zum Fragenkatalog im Rahmen der Anhörung des Ausschusses für Kommunale Fragen, Innere Sicherheit und Sport zum Gesetzentwurf zur Änderung des Polizeiaufgabengesetzes und weiterer Rechtsvorschriften am 16. Mai 2024 – **Anlage 11**, S. 14, 18 ff.; *Zöller*, Schriftliche Stellungnahme zum Gesetzentwurf der Staatsregierung für ein Gesetz zur Änderung des Polizeiaufgabengesetzes und weiterer Rechtsvorschriften vom 9. April 2024 (LT-Drs. 19/1557) – **Anlage 12**, S. 16.

Die in Art. 61a Abs. 2 Satz 1 i.V.m. Abs. 1 Satz 1 BayPAG vorgesehenen Maßnahmen bewegen sich noch im Vorfeld einer konkretisierten Gefahr und genügen daher den Anforderungen des angerufenen Gerichtes nicht,

> so auch zu dem Gesetzentwurf, der, bis auf kleinste Änderungen, der nun geltenden Regelung entspricht *Petri*, Stellungnahme zum Fragenkatalog im Rahmen der Anhörung des Ausschusses für Kommu-

nale Fragen, Innere Sicherheit und Sport zum Gesetzentwurf zur Änderung des Polizeiaufgabengesetzes und weiterer Rechtsvorschriften am 16. Mai 2024 – **Anlage 11**, S. 18 ff.

aaa. Art. 61a Abs. 2 Satz 1 Nr. 1 BayPAG

(1) Eingriffsschwelle

Die vorgesehene Eingriffsschwelle genügt den verfassungsrechtlichen Anforderungen nicht. Die in Art. 61a Abs. 2 Satz 1 Nr. 1 BayPAG geregelte Eingriffsschwelle deckt sich nicht mit den vom angerufenen Gericht gestellten Anforderungen an eine konkretisierte Gefahr (siehe hierzu **D.II.1.a.aa.aaa.**).

Der bayerische Gesetzgeber lässt es in Art. 61a Abs. 2 Satz 1 Nr. 1 BayPAG ausreichen, „wenn aufgrund tatsächlicher Anhaltspunkte innerhalb eines übersehbaren Zeitraums mit weiteren gleichgelagerten Straftaten zu rechnen ist“. Damit regelt die Eingriffsgrundlage mit dem Erfordernis eines auf bestimmten Tatsachen beruhenden konkretisierten und zeitlich absehbaren Geschehens nur die erste Voraussetzung der konkretisierten Gefahr.

Der zweite Aspekt einer konkretisierten Gefahr, nämlich dass sich die Prognose auch darauf beziehen muss, 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, ist in der Definition nicht enthalten. Insofern bleibt Art. 61a Abs. 2 Satz 1 Nr. 1 BayPAG hinter den verfassungsrechtlichen Anforderungen zurück.

Auch im Rahmen des Art. 61a Abs. 2 Satz 1 Nr. 1 BayPAG kann diese Schwelle aus den bereits oben dargestellten Gründen (siehe **D.II.1.a.bb.bbb.(2)(b)**) nicht durch eine Heranziehung der Art. 7 ff. BayPAG personell konkretisiert werden.

(2) Unzulässiger dynamischer Verweis auf § 100b Abs. 2 StPO

Zudem ist die dynamische Verweisung auf § 100b Abs. 2 StPO in Art. 61a Abs. 2 Satz 1 Nr. 1 BayPAG schon ihrer Form nach nicht mit verfassungsrechtlichen Anforderungen an Bestimmtheit und Normenklarheit (siehe dazu **D.I.1.a.bb.bbb.**) vereinbar,

> BVerfGE 162, 1 (169 Rn. 383 ff.) ebenfalls zu einer Verweisung auf § 100b Abs. 2 StPO in einer sicherheitsrechtlichen Ermächtigungsgrundlage (Art. 8b Abs. 2 BayVSG a.F.).

Der gesetzgeberischen Begründung ist nicht zu entnehmen, dass auf § 100b Abs. 2 StPO nur in seiner aktuellen bundesgesetzlichen Fassung verwiesen werden soll. Vielmehr wird § 100b Abs. 2 StPO pauschal in Bezug genommen,

> vgl. LT-Drs. 19/1557, S. 26.

Es handelt sich mithin um eine dynamische Verweisung. Eine solche unterliegt besonderen verfassungsrechtlichen Anforderungen (siehe hierzu **D.I.1.a.bb.bbb.(2)**), welche vorliegend nicht gewahrt sind.

Art. 61a Abs. 2 Satz 1 Nr. 1 BayPAG ist Rechtsgrundlage für automatisierte Datenanalysen, bei denen es sich gerade um eigenständige und schwerwiegende Grundrechtseingriffe handelt. Bei Schaffung einer Rechtsgrundlage für diese Eingriffe bedarf es daher einer vollständigen Abwägung der einschlägigen Grundrechte mit kollidierenden Grundrechten und anderen Verfassungsgütern und Interessen durch den bayerischen Landesgesetzgeber selbst,

> BVerfGE 162, 1 (170 Rn. 386 m.w.N).

Dies geschieht nicht in erforderlicher Weise, wenn § 100b Abs. 2 StPO in Bezug genommen wird. Hiermit übernimmt der Landesgesetzgeber für die Abwägungsentscheidung, welche Straftaten er als Anknüpfungspunkte für die Tatbestandsvoraussetzungen und damit für die Rechtfertigung der Datenanalyse genügen lassen will, dynamisch eine fremde Abwägungsent-

scheidung des Bundesgesetzgebers. Da der Bund diese Norm jedoch jederzeit verändern kann, kann der Gesetzgeber deren Gewicht nicht kennen und daher auch nicht in seine Abwägung einstellen,

> BVerfGE 162, 1 (170 Rn. 386 m.w.N.) zu einem dynamischen Verweis auf § 100b Abs. 2 StPO in einer sicherheitsrechtlichen Ermächtigungsgrundlage.

Die dynamische Verweisung ist auch nicht ausnahmsweise zulässig, weil § 100b Abs. 2 StPO gerade kein eng umrissenes Feld regelt, dessen Inhalt weitgehend feststünde,

> BVerfGE 162, 1 (170 Rn. 386 m.w.N.) zu einem dynamischen Verweis auf § 100b Abs. 2 StPO in einer sicherheitsrechtlichen Ermächtigungsgrundlage.

Der 2017 geschaffene § 100b StPO wurde bereits 2021 deutlich verändert,

> BGBl. I S. 2099 (2102).

Dies geschah laut Gesetzesbegründung, um die Norm an die Bedürfnisse der Praxis anzupassen. Dabei wurden Delikte zum Schutz völlig unterschiedlicher Rechtsgüter aufgenommen, vom gewerbs- und bandenmäßigen Computerbetrug gemäß § 263a StGB über Delikte im Bereich des Menschenhandels bis zu Delikten aus Spezialgesetzen wie dem Außenwirtschaftsgesetz (AWG), dem Grundstoffüberwachungsgesetz (GÜG) und dem Neue-psychoaktive-Stoffe-Gesetz (NpSG),

> BT-Drs. 57/27, S. 35 f.

Da das Sicherheitsrecht ein Feld intensiver politischer Auseinandersetzung ist, sind weitere Änderungen des Katalogs in § 100b Abs. 2 StPO schwer abzusehen,

> BVerfGE 162, 1 (170 Rn. 386 m.w.N.) zu einem dynamischen Verweis auf § 100b Abs. 2 StPO in einer sicherheitsrechtlichen Ermächtigungsgrundlage.

Dies zeigt sich bereits an den vielfach geplanten Änderungen des Sicherheitsrechts im aktuellen Koalitionsvertrag der neuen Bundesregierung,

der zahlreiche neue Befugnisse bzw. Erweiterungen bereits bestehender sicherheitsbehördlicher Befugnisse vorsieht,

> Verantwortung für Deutschland, Koalitionsvertrag zwischen CDU, CSU und SPD, 21. Legislaturperiode, https://www.koalitionsvertrag2025.de/, (82 Zl. 2629 ff.).

Auch kann eine Zulässigkeit der dynamischen Verweisung auf § 100b Abs. 2 StPO nicht daraus gefolgert werden, dass das angerufene Gericht selbst im Rahmen seiner befristeten Anordnung der Fortgeltung der verfassungswidrigen hessischen Ermächtigungsgrundlagen für die automatisierte Datenanalyse 2023 ebenfalls auf § 100b Abs. 2 StPO verwies,

> BVerfGE 165, 363 (440 Rn. 176), a.A. LT-Drs. 19/1557, S. 26.

Für die Übergangszeit bis zur Schaffung neuer verfassungskonformer Rechtsgrundlagen wurde die hessische Regelung dergestalt eingeschränkt, dass von der Befugnis zur Datenanalyse nur bei einem auf bestimmte, genügend konkretisierte Tatsachen begründeten Verdacht einer Straftat nach § 100b Abs. 2 StPO Gebrauch gemacht werden sollte, wenn aufgrund der konkreten Umstände eines solchen im Einzelfall bestehenden Tatverdachts für die Zukunft mit weiteren, gleichgelagerten Straftaten zu rechnen wäre, die Leib, Leben oder den Bestand oder die Sicherheit des Bundes oder eines Landes gefährden,

> BVerfGE 165, 363 (440 Rn. 176).

Hierbei handelte es sich nicht um eine vollständige normsetzende Abwägung des Eingriffsgewichts und der Rechtfertigungsvoraussetzungen durch den Gesetzgeber, sondern um eine Einschränkung im Rahmen einer bloß eng befristeten Anordnung der Fortgeltung verfassungswidriger Rechtsgrundlagen,

> BVerfGE 165, 363 (440 Rn. 176).

Diese sollte den Gesetzgeber gerade nicht präjudizieren, sondern lediglich die betroffenen Grundrechte schützen und bis zur Herstellung verfassungsmäßiger Zustände durch den Gesetzgeber die Befugnisse auf das reduzieren, was nach Maßgabe dieser Abwägung geboten ist,

BVerfGE 165, 363 (440 Rn. 176); BVerfGE 141, 220 (351 Rn. 355 m.w.N.).

Es handelt sich lediglich um eine Übergangsregelung.

Für diese Anordnung müssen schon wegen ihrer begrenzten zeitlichen Dauer von sechs Monaten und dem damit deutlich geringeren Risiko einer Veränderung der dynamischen Verweisung andere Maßstäbe zugrunde gelegt werden. Die Vorgaben können daher nicht ohne Weiteres als verfassungskonforme Abwägungsergebnisse einer gesetzgeberischen Grundrechtsabwägung verstanden werden.

Einer verfassungskonformen Auslegung der Norm (zum Maßstab bereits **D.II.1.a.bb.bbb.(1)(b)(aa)**) in eine statische Verweisung,

BVerfGE 162, 1 (171 Rn. 387),

steht zum einen entgegen, dass der Gesetzgeber bewusst keine weiteren Einschränkungen als den Verweis auf § 100b StPO aufgenommen hat, den er fälschlicherweise unter Bezugnahme der dargestellten Übergangsregelung als ausreichend erachtete. Dabei wurde die gegenüber Bayern ergangene Entscheidung zur Unzulässigkeit einer dynamischen Verweisung auf § 100b Abs. 2 StPO schlicht ignoriert.

Eine verfassungskonforme Auslegung als statische Verweisung würde auch hier dem bayerischen Gesetzgeber die Verantwortung abnehmen, eine eigene Grundrechtsabwägung vorzunehmen, deren Ergebnis den verfassungsrechtlichen Anforderungen genügt, statt trotz bereits ergangener Rechtsprechung zu einer dynamischen Verweisung auf § 100b Abs. 2 StPO erneut bestimmtheitswidrig auf diese bundesgesetzliche Norm zu verweisen.

Da vorliegend aber die in § 100b Abs. 2 StPO enthaltenen Straftaten den Anforderungen an die Eingriffsschwelle für die Rechtfertigung eines besonders schweren Grundrechtseingriffes gerade nicht genügen, da sie nicht nur besonders gewichtige Rechtsgüter schützen, kann auch eine solche Auslegung als statische Verweisung die Verfassungswidrigkeit der Norm nicht heilen.

(3) Zu schützende Rechtsgüter

Der Katalog des § 100b Abs. 2 StPO ist verfassungsrechtlich nicht tragfähig, weil er auch Straftaten enthält, die nicht die durch das angerufene Gericht eng begrenzten besonders gewichtigen Rechtsgüter (siehe hierzu **(D.II.1.a.aa.bbb.)**) schützen (dazu **(a)**). Selbst wenn man auch eine Anknüpfung an andere besonders schwere Straftaten als ausreichend erachtete, enthielte der Katalog nicht nur besonders schwere Straftaten (dazu **(b)**). Zudem knüpft der Katalog in verfassungswidriger Weise an Vorfeldstraftaten an (dazu **(c)**).

(a) Kein Schutz besonders gewichtiger Rechtsgüter

Art. 61a Abs. 2 Satz 1 Nr. 1 BayPAG knüpft mit seinem Verweis auf § 100b Abs. 2 StPO nicht an die Gefährdung besonders gewichtiger Rechtsgüter an.

Soweit das angerufene Gericht im nachrichtendienstlichen Kontext als Anknüpfungspunkte besonders schwere Straftaten genügen lässt, ohne dass diese besonders gewichtige Rechtsgüter betreffen müssen, sind diese Maßstäbe vorliegend nicht zu übertragen. Nach diesen Maßstäben sind dann, wenn der Gesetzgeber den Eingriffstatbestand durch eine Bezugnahme auf Straftatbestände konturiert, die Gewichtungen entsprechend heranzuziehen, die für die strafprozessuale Datenerhebung gelten. Zwischen der präventiven und der repressiven Anknüpfung an Straftaten bestehe ein Gleichlauf,

> vgl. zu Übermittlungsermächtigungen BVerfGE 163, 43 (93 R. 131); 162, 1 (115 Rn. 244).

Nach diesem Maßstab entspricht einer Gefährdung eines Rechtsguts von herausragendem öffentlichem Interesse eine Begrenzung auf besonders schwere Straftaten,

> BVerfGE 162, 1 (115 Rn. 244).

Eine Übertragung dieser Grundsätze führt zu einer inkohärenten Aufspaltung der verfassungsrechtlichen Anforderungen an präventivpolizeiliche

Überwachungsermächtigungen. Sie eröffnet dem Gesetzgeber die Möglichkeit, die strengen Anforderungen an das zu schützende Rechtsgut zu umgehen, indem er den Eingriffstatbestand durch Bezugnahme auf Straftaten gestaltet.

Zugleich steht dem Gesetzgeber die Entscheidung über den gesetzlichen Strafrahmen weitgehend frei. So könnte der Gesetzgeber weitreichende Überwachungsermächtigungen ermöglichen, indem er schlicht die gesetzlichen Strafrahmen einschlägiger Delikte weitgehend ohne Rücksicht auf deren Schutzgüter erhöht.

Es ist daher weiterhin zu fordern, dass eine Straftat nur dann als Anknüpfungspunkt für eine tief in die Grundrechte eingreifende heimliche Ermittlungsmaßnahme herangezogen werden kann, wenn sie dem Schutz eines besonders gewichtigen Rechtsguts dient,

> so auch BVerwG, Beschluss vom 31. Mai 2022, BVerwG 6 C 2.20, Rn. 33.

Dies entspricht auch den Anforderungen, die das angerufene Gericht selbst im Rahmen seiner befristeten Anordnung der Fortgeltung der verfassungswidrigen hessischen Ermächtigungsgrundlagen für die automatisierte Datenanalyse 2023 an den Verweis auf § 100b Abs. 2 StPO stellte.

Für die Übergangszeit bis zur Schaffung neuer verfassungskonformer Rechtsgrundlagen wurde die hessische Regelung dergestalt eingeschränkt, dass von der Befugnis zur Datenanalyse nur bei einem auf bestimmte, genügend konkretisierten Tatsachen begründeten Verdacht einer Straftat nach § 100b Abs. 2 StPO zulässig sein sollte, wenn aufgrund der konkreten Umstände eines solchen im Einzelfall bestehenden Tatverdachts für die Zukunft mit weiteren, gleichgelagerten Straftaten zu rechnen wäre, die Leib, Leben oder den Bestand oder die Sicherheit des Bundes oder eines Landes gefährden,

> BVerfGE 165, 363 (440 Rn. 176).

Die im Katalog des § 100b Abs. 2 StPO genannten Straftatbestände dienen zwar teilweise auch dem Schutz besonders gewichtiger Rechtsgüter im

Sinne der Rechtsprechung des angerufenen Gerichts. Jedoch gilt das nicht für alle dort genannten Strafnormen,

> so auch zu dem Gesetzentwurf, der, bis auf kleinste Änderungen, der nun geltenden Regelung entspricht *Petri*, Stellungnahme zum Fragenkatalog im Rahmen der Anhörung des Ausschusses für Kommunale Fragen, Innere Sicherheit und Sport zum Gesetzentwurf zur Änderung des Polizeiaufgabengesetzes und weiterer Rechtsvorschriften am 16. Mai 2024 – **Anlage 11,** S. 19.

Insbesondere knüpft § 100b Abs. 2 StPO in seinem Katalog auch an eine Vielzahl von Delikten an, die primär Vermögen oder Eigentum schützen, obwohl bedeutsame Sachwerte nur in den durch das angerufene Gericht definierten engen Grenzen („wesentliche Infrastruktureinrichtungen oder sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen […]“) ein zulässiges Schutzgut darstellen,

> BVerfGE 165, 363 (410 Rn. 105); 141, 220 (287 f. Rn. 155).

Damit sind die folgenden Delikte nicht als besonders schwere Straftaten anzusehen:

- § 100b Abs. 2 Nr. 1 lit. d) StPO (Geld- und Wertzeichenfälschungen)
- § 100b Abs. 2 Nr. 1 lit. i) StPO (Bandendiebstahl)
- § 100b Abs. 2 Nr. 1 lit. j) StPO (jedenfalls hinsichtlich des schweren Raubes, § 250 Abs. 1, 2 StPO, soweit es nicht tateinheitlich zu Körperverletzungen kam)
- § 100b Abs. 2 Nr. 1 lit. k) StPO (räuberische Erpressung und besonders schwerer Fall der Erpressung, soweit es nicht tateinheitlich zu Körperverletzungen kam)
- § 100b Abs. 2 Nr. 1 lit. l) StPO (Qualifikationen der Hehlerei)
- § 100b Abs. 2 Nr. 1 lit. m) StPO (Geldwäsche)
- § 100b Abs. 2 Nr. 1 lit. n) StPO (Computerbetrug)
- § 100b Abs. 2 Nr. 1 lit. b) StPO (Betrieb krimineller Handelsplattformen, sofern sich lit. b) auf die zuvor genannten Ziffern und Straftaten bezieht).

Ebenso wenig genügen Verstöße gegen Asyl- und Aufenthaltsgesetz, sodass § 100b Abs. 2 Nr. 2 und 3 StPO keine besonders schweren Straftaten beinhalten.

Eine andere Beurteilung der Straftaten in § 100b Abs. 2 StPO hinsichtlich der geschützten Rechtsgüter folgt auch hier nicht daraus, dass das angerufene Gericht selbst im Rahmen seiner befristeten Anordnung der Fortgeltung der verfassungswidrigen hessischen Ermächtigungsgrundlage im Datenanalyseurteil ebenfalls auf § 100b Abs. 2 StPO verwies,

> BVerfGE 165, 363 (440 Rn. 176), a.A. LT-Drs. 19/1557, S. 26.

Dem kann gerade nicht entnommen werden, dass allein ein Verweis auf den Katalog des § 100b Abs. 2 StPO durch den Gesetzgeber zum dauerhaften Schutz der Grundrechte genügen würde und dass der Katalog zum Schutz besonders wichtiger Rechtsgüter genügt, da das angerufene Gericht die Gefährdung besonders gewichtiger Rechtsgüter ausdrücklich neben der Gefahr einer Straftat nach § 100b Abs. 2 StPO gefordert hat.

Das angerufene Gericht hat vielmehr zuletzt in einer Entscheidung mangels Entscheidungserheblichkeit offengelassen, ob § 100b Abs. 2 StPO hinreichend gewichtige Rechtsgüter und Schwellen vorsieht,

> BVerfGE 162, 1 (172 Rn. 388).

Die bayerische Polizei setzt die Analysesoftware „VeRA“ auf Grundlage von Art. 61a Abs. 2 Satz 1 Nr. 1 BayPAG vielfach auch zum Schutz vor Straftaten im Sinne des § 100b Abs. 2 StPO ein,

> Anfragen zum Plenum (zur Plenarsitzung am 21. Mai 2025) mit den dazu eingegangenen Antworten der Staatsregierung, LT-Drs. 19/6865, S. 2 f.; Präsidentin des Bayerischen Landtags, Antwort auf die schriftliche Anfrage des Abgeordneten Benjamin Adjei vom 28.04.2025 betreffend Einsatz und Betrieb der polizeilichen Analyseplattform VeRA, **Anlage 13**, S. 2 ff.

(b) Keine besonders schweren Straftaten im Übrigen

Selbst wenn das angerufene Gericht davon ausginge, zum Schutz überragend wichtiger Rechtsgüter genüge, wenn der Gesetzgeber an besonders schwere Straftaten anknüpfe, würde der Verweis auf § 100b Abs .2 StPO auch diesen Anforderungen nicht genügen.

Knüpft der Gesetzgeber zur Beschreibung des Schutzguts statt an besonders gewichtige Rechtsgüter an drohende Straftaten an, so muss es sich um besonders schwere Straftaten handeln. Als besonders schwere Straftaten werden zumindest in erster Linie solche angesehen, die mit einer Höchststrafe von mehr als fünf Jahren bedroht sind,

BVerfGE 169, 130 (219 Rn. 203); 165, 1 (93 Rn. 179).

Ein Höchststrafrahmen von mindestens fünf Jahren hingegen qualifiziert eine Straftat weder als schwer noch als besonders schwer,

BVerfGE 169, 130 (219 Rn. 204).

Der Strafrahmen hat zwar eine Indizwirkung für die Beurteilung der besonderen Schwere einer Straftat, eine Straftat mit einer angedrohten Höchstfreiheitsstrafe von fünf Jahren kann aber auch dann als besonders schwer eingestuft werden, wenn dies „nicht nur unter Berücksichtigung des jeweils geschützten Rechtsguts und dessen Bedeutung für die Rechtsgemeinschaft, sondern auch unter Berücksichtigung der Tatbegehung und Tatfolgen vertretbar erscheint“,

BVerfGE 169, 130 (219 Rn. 205).

Die Qualifizierung als besonders schwere Straftat muss in der Strafnorm selbst einen objektivierten Ausdruck finden, insbesondere im Strafrahmen und ggf. in tatbestandlich umschriebenen oder in einem Qualifikationstatbestand enthaltenen Begehungsmerkmalen und Tatfolgen,

BVerfGE 169, 130 (220 Rn. 206).

Für Wohnraumüberwachungen und Online-Durchsuchungen hat das angerufene Gericht einen Strafrahmen mit Höchstfreiheitsstrafe von mindestens fünf Jahren nicht ausreichen lassen,

BVerfGE 169, 130 (219 Rn. 205); 141, 220 (338 Rn. 316).

Jedenfalls keine besonders schweren Straftaten in diesem Sinne sind Delikte, die lediglich einen Strafrahmen von bis zu drei Jahren Freiheitsstrafe oder Geldstrafe vorsehen,

vgl. BVerfGE 169, 130 (219 Rn. 205); 163, 43 (102 Rn. 155); 165, 1 (93 Rn. 180).

Auch unter Anwendung dieses Maßstabs genügt § 100b Abs. 2 StPO den verfassungsrechtlichen Anforderungen nicht.

Dies ergibt sich zum einen daraus, dass § 100b StPO umfänglich, teils ausdrücklich, auf minder schwere Fälle verweist, deren Einstufung als besonders schwere Straftaten weder ihrem Strafmaß nach indiziert ist noch im Tatbestand der Norm einen den Vorgaben entsprechenden objektivierten Ausdruck findet. Minder schwere Fälle, die im Höchstmaß mit Freiheitsstrafe von 5 Jahren bestraft sind, finden sich in den § 82 Abs. 2 StGB, § 89a Abs. 5 StGB, § 100 Abs. 3 StGB, § 146 Abs. 3 StGB, § 152b Abs. 3 StGB, § 234 Abs. 2 StGB, § 234a Abs. 2 StGB (explizite gesetzliche Inbezugnahme), § 244a Abs. 2 StGB, § 260a Abs. 2 StGB, § 263 Abs. 5 StGB, § 84a Abs. 2 AsylG und § 29a Abs. 2 BtMG.

Dass der Gesetzgeber bewusst auch die Begehungsgefahr dieser minder schweren Fälle als Eingriffsschwelle ausreichen lassen wollte, ergibt sich nicht zuletzt daraus, dass in einigen Verweisungsnormen Bezugnahmen auf diejenigen Absätze, die einen minder schweren Fall regeln, dezidiert ausgespart wurden, etwa § 89c Abs. 5 StGB, § 233a Abs. 4 Halbsatz 1 StGB oder § 30 Abs. 2 BtMG. Im Übrigen wird bezüglich vieler anderer Straftaten von vornherein auf besonders schwere Fälle verwiesen, etwa in den § 95 Abs. 3 StGB, § 98 Abs. 1 Satz 2 StGB oder § 99 Abs. 2 StGB.

Erreichen diese minder schweren Fälle aber nicht den verfassungsrechtlich vorgegebenen Höchststrafrahmen, erscheint ihre Einstufung als besonders schwere Straftaten in fast allen Fällen auch unter Berücksichtigung der jeweils geschützten Rechtsgüter und deren Bedeutung für die

Rechtsgemeinschaft sowie der erfassten Tatbegehung und der Tatfolgen nicht vertretbar.

Hier seien dafür nur einige Beispiele herausgegriffen: Über § 100b Abs. 2 Nr. 1 lit. d) StPO ist beispielsweise auf die Geld- oder Wertpapierfälschung in einem minder schweren Fall gemäß § 146 Abs. 3 StGB bzw. § 151 StGB verwiesen. Nach der eigenen Wertung des Gesetzgebers kann für eine solche Tatbegehung schon eine Strafe von drei Monaten Freiheitsstrafe ausreichen. Eine besonders schwere Art der Tatbegehung oder besonders schwere Tatfolgen sind nicht ersichtlich, finden aber jedenfalls in der Strafnorm selbst keinen objektivierenden Ausdruck. Konkret würde also beispielsweise schon die Gefahr der Herstellung geringfügigster Mengen von Falschgeld, beispielsweise auch nur eines einzelnen Scheins, ausreichen, um automatisierte Datenanalysen nach Art. 61a Abs. 2 Satz 1 Nr. 1 BayPAG zu ermöglichen.

Ähnliche Ungleichgewichte können beim Verdacht der gewerbsmäßigen Bandenhehlerei gemäß § 260a StGB entstehen, die im minder schweren Fall gemäß § 260a Abs. 2 StGB mit einer Freiheitsstrafe von sechs Monaten bis fünf Jahren bestraft wird. Auch hier zeigt die Aufnahme eines minder schweren Falles an, dass der Gesetzgeber selbst nicht davon ausgeht, dass es sich notwendigerweise um eine besonders schwere Straftat handelt. Zuletzt genannt sei auch noch § 29a BtMG, im minder schweren Fall gemäß Abs. 2 wiederum mit einer Mindestfreiheitsstrafe von drei Monaten bestraft. Erfasst ist danach auch schon der Besitz von Betäubungsmitteln in nicht geringer Menge in einem minder schweren Fall.

(c) Unzulässige Anknüpfung an Vorfeldstrafbarkeiten

Darüber hinaus verweist § 100b Abs. 2 Nr. 1 lit. a), b) und c) StPO auf strafrechtliche Vorfeldtatbestände wie § 89a oder § 129a StGB, für deren Verwirklichung der Gesetzgeber an Vorfeldhandlungen anknüpft.

Damit an die Begehung solcher Vorfeldstrafbarkeiten als Anlass angeknüpft werden kann, muss der Gesetzgeber zusätzlich sicherstellen, dass Maßnahmen nur zulässig sind, wenn mit der Begehung solcher Straftaten

bereits eine konkretisierte Gefahr für das durch den Tatbestand geschützte Rechtsgut vorliegt,

BVerfGE 165, 363 (438 f. Rn. 170) m.w.N.

Diesen Anforderungen entsprechen die in § 100b StPO in Bezug genommenen Straftatbestände nicht in allen Fällen. Über § 100b Abs. 2 Nr. 1 lit. a), b) und c) StPO wird auch auf Delikte verwiesen, bei denen die Strafbarkeitsschwelle durch die Einbeziehung von Vorbereitungshandlungen in das Vorfeld von konkreten Rechtsgutsgefahren oder -verletzungen verlagert ist. Dazu gehören zum einen die Vorbereitung einer schweren staatsgefährdenden Gewalttat gemäß § 89a StGB und die Terrorismusfinanzierung gemäß § 89c Abs. 1-4 StGB, zum anderen friedensgefährdende Beziehungen gemäß § 100 StGB und die Bildung krimineller Vereinigungen in einem besonders schweren Fall gemäß § 129 Abs. 5 StGB sowie terroristischer Vereinigungen gemäß § 129a StGB. Auch wenn es sich bei diesen Straftaten teils um schwere Delikte handelt, so steht nach der verfassungsgerichtlichen Rechtsprechung doch fest, dass ihre vermutete Begehung eben nur dann zu den entsprechenden Eingriffen führen darf, wenn eine konkretisierte oder konkrete Gefahr für das durch den Straftatbestand geschützte Rechtsgut besteht. Da Art. 61a Abs. 2 Satz 1 Nr. 1 BayPAG aber keine derartige zureichende Gefahrenschwelle vorsieht, ist auch diesem verfassungsrechtlichen Erfordernis nicht entsprochen. Eine konkrete Rechtsgutsgefährdung wird nämlich auch durch den Zusatz „wenn aufgrund tatsächlicher Anhaltspunkte innerhalb eines übersehbaren Zeitraums mit weiteren gleichgelagerten Straftaten zu rechnen ist“ nicht vorausgesetzt, da insofern ja wiederum bereits die Begehung eines Vorfelddelikts ausreichend ist.

bbb. Art. 61a Abs. 2 Satz Nr. 2 BayPAG

Art. 61a Abs. 2 Satz 1 Nr. 2 BayPAG genügt den verfassungsrechtlichen Anforderungen an Rechtsgüterschutz und Eingriffsschwelle nicht, da die Tatbestandsvariante nicht nur besonders wichtige Rechtsgüter in Bezug nimmt (dazu **(1)**) und einen Eingriff unterhalb der konkretisierten Gefahr im Gefahrenvorfeld zulässt (dazu **(2)**),

so auch zu dem Gesetzentwurf, der, bis auf kleinste Änderungen, der nun geltenden Regelung entspricht *Petri*, Stellungnahme zum Fragenkatalog im Rahmen der Anhörung des Ausschusses für Kommunale Fragen, Innere Sicherheit und Sport zum Gesetzentwurf zur Änderung des Polizeiaufgabengesetzes und weiterer Rechtsvorschriften am 16. Mai 2024 – **Anlage 11**, S. 19 f.

(1) Zu schützende Rechtsgüter

Art. 61a Abs. 2 Satz 1 Nr. 2 BayPAG setzt bereits die zu schützenden Rechtsgüter zu gering an, die zudem nicht hinreichend bestimmt und normenklar geregelt sind. Dies gilt insbesondere für Art. 61a Abs. 1 Satz 1 Nr. 2 lit. c) (dazu **(a)**) und lit. d) BayPAG (dazu **(b)**).

Art. 61a Abs. 2 Satz 1 Nr. 2 BayPAG knüpft die automatisierte Datenanalyse nicht an besonders gewichtige Rechtsgüter an,

zu dem Gesetzentwurf, der, bis auf kleinste Änderungen, der nun geltenden Regelung entspricht *Zöller*, Schriftliche Stellungnahme zum Gesetzentwurf der Staatsregierung für ein Gesetz zur Änderung des Polizeiaufgabengesetzes und weiterer Rechtsvorschriften vom 9. April 2024 (LT-Drs. 19/1557) – **Anlage 12**, S. 17; a.A. *Aulehner* in: BeckOK/PolR Bayern, 25. Ed. 15.10.2024, PAG Art. 61a, Rn. 29 f.

Die gesetzlich genannten Rechtsgüter sind überdies zu unbestimmt und verletzen den Grundsatz der Normenklarheit. Der Gesetzeswortlaut enthält eine Vielzahl unbestimmter Rechtsbegriffe, welche auch mit den gängigen Auslegungsmethoden nicht ausreichend bestimmbar sind,

zu dem Gesetzentwurf, der, bis auf kleinste Änderungen, der nun geltenden Regelung entspricht *Zöller*, Schriftliche Stellungnahme zum Gesetzentwurf der Staatsregierung für ein Gesetz zur Änderung des Polizeiaufgabengesetzes und weiterer Rechtsvorschriften vom 9. April 2024 (LT-Drs. 19/1557) – **Anlage 12**, S. 16.

Die genannten Rechtsgüter genügen mithin nicht den verfassungsrechtlichen Anforderungen, die an besonders gewichtige Rechtsgüter zu stellen sind (siehe hierzu **(D.II.1.a.aa.bbb.)**).

Der Gesetzgeber erkennt selbst, dass die in Art. 61a Abs. 2 Satz 2 Nr. 2 genannten Rechtsgüter nicht als besonders wichtig anzusehen sind und dass daher eine Senkung des Eingriffsgewichts der Datenanalyse nach Absatz 2 erforderlich ist,

> LT-Drs. 19/1557, S. 26.

Der Gesetzgeber geht aber – unzutreffend – von einem geringeren Eingriffsgewicht der Datenanalyse nach Art. 61a Abs. 2 BayPAG aus, welches die Absenkung des Gewichts der zu schützenden Rechtsgüter rechtfertigen würde.

Schon Art. 61a Abs. 2 Satz 1 Nr. 2 lit. a) BayPAG knüpft explizit an die Verletzung der Gesundheit einer Person an, soweit keine Gefahr im Sinne des Abs. 1 Satz 1 Nr. 1 gegeben ist. Schon diese Einschränkung spricht dafür, dass die Rechtsgüter nicht ausreichend wichtig sind,

> so auch zu dem Gesetzentwurf, der, bis auf kleinste Änderungen, der nun geltenden Regelung entspricht *Petri*, Stellungnahme zum Fragenkatalog im Rahmen der Anhörung des Ausschusses für Kommunale Fragen, Innere Sicherheit und Sport zum Gesetzentwurf zur Änderung des Polizeiaufgabengesetzes und weiterer Rechtsvorschriften am 16. Mai 2024 – **Anlage 11,** S. 19.

In besonderer Weise genügen jedoch Art. 61a Abs 1 Satz 1 Nr. 2 lit. c) (dazu **(a)**) und lit. d) BayPAG (dazu **(b)**) nicht den verfassungsrechtlichen Anforderungen.

(a) Art. 61a Abs. 1 Satz 1 Nr. 2 lit. c) BayPAG

Art. 61a Abs. 1 Satz 1 Nr. 2 lit. c) BayPAG schützt keine besonders gewichtigen Rechtsgüter. Nicht alle Eigentums- und Vermögenswerte sind, auch wenn sie durch gewerbsmäßig oder bandenmäßig begangene Straftaten gefährdet werden und diese geeignet sind, den Rechtsfrieden in erheblicher Weise zu stören, als besonders gewichtige Rechtsgüter einzustufen,

> so auch zu dem Gesetzentwurf, der, bis auf kleinste Änderungen, der nun geltenden Regelung entspricht *Petri*, Stellungnahme zum Fra-

genkatalog im Rahmen der Anhörung des Ausschusses für Kommunale Fragen, Innere Sicherheit und Sport zum Gesetzentwurf zur Änderung des Polizeiaufgabengesetzes und weiterer Rechtsvorschriften am 16. Mai 2024 – **Anlage 11**, S. 19.

Zudem genügt die in der Norm vorgesehene Eignung zur Störung des Rechtsfriedens nicht den Anforderungen an Bestimmtheit und Normenklarheit.

Das angerufene Gericht hat explizit klargestellt, dass Sachwerte nur in engen Grenzen überragend wichtige Rechtsgüter darstellen können (dazu **D.II.1.a.aa.bbb.**). Diese Grenzen sind vorliegend nicht eingehalten.

Unter Art. 61a Abs. 2 Satz 1 Nr. 2 lit. c) BayPAG können auch Gefahren fallen, die Sachwerte betreffen, die nicht Infrastruktureinrichtungen oder sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen sind. Vielmehr können schon gewerbsmäßige Fahrraddiebstähle oder Betrugsdelikte ausreichen.

Dem kann auch nicht entgegengehalten werden, die Norm ziele nicht auf Eigentum als Rechtsgut, sondern auf einen besonders erheblichen Modus Operandi der Verletzung bei gewerbsmäßiger und bandenmäßiger Begehung,

so aber *Benamor*, BayVBl 2025, 44 (47).

Diese Abstufung des Rechtsgüterschutzes nicht in Bezug auf die Wertigkeit des Rechtsguts ist mit Blick auf das hohe Eingriffsgewicht heimlicher Überwachungsmaßnahmen nicht angezeigt. Die Begehungsweise bzw. die Art und Weise der Rechtsgutsverletzung kann allein nicht zur Annahme von besonders wichtigen Rechtsgütern führen.

Zudem ist das Erfordernis der Eignung zur erheblichen Störung des Rechtsfriedens in Art. 61a Abs. 2 Satz 1 Nr. 2 lit. c) BayPAG in seinen Grenzen für die normanwendenden Personen nicht hinreichend bestimmt und lassen zu große Spielräume, die nicht mit den gängigen Auslegungsmethoden geschlossen werden können.

Das Tatbestandsmerkmal lässt Raum für nicht nachvollziehbare Bewertungen und Einschätzungen im Einzelfall und ist nicht hinreichend konturiert. Es bietet normanwendenden Polizist*innen und Gerichten keine ausreichenden Anhaltspunkte für die Auslegung.

Jedenfalls für Bürger*innen, die ihr Verhalten an der Norm ausrichten wollen, ist die Begrenzung auf solche Straftaten, die geeignet sind, den Rechtsfrieden erheblich zu stören, nicht nachvollziehbar.

Die Eignung zur erheblichen Störung des Rechtsfriedens ist ein weites und im Einzelfall nicht trennscharfes Kriterium. Dies gilt umso mehr, weil in der Gesetzesbegründung das Merkmal insbesondere auf organisierte Kriminalität im Bereich „regelmäßig schwerwiegender Delikte aus dem Bereich der Vermögens- und Eigentumskriminalität“ fokussiert ist,

> LT-Drs. 19/1557, S. 26 a.E.

Damit vermischt der Gesetzgeber die Tatbestandsmerkmale der „Eigentums- und Vermögenswerte, wenn tatsächliche Anhaltspunkte für eine drohende gewerbsmäßige oder bandenmäßige Schädigung dieser Rechtsgüter vorliegen“ mit dem Merkmal der Eignung zur erheblichen Störung des Rechtsfriedens. Gerade die Organisiertheit oder die Begehung von Vermögens- und Eigentumsdelikten stellen eigene Tatbestandsmerkmale dar. Dürften diese nochmals zur Erfüllung der Eignung der Störung des Rechtsfriedens herangezogen werden, käme dem Tatbestandsmerkmal für diese keine eigene Bedeutung zu. Dies gilt insbesondere, weil bereits die Eignung zur Störung des Rechtsfriedens genügt, eine tatsächliche Störung des Rechtsfriedens also nicht erforderlich ist.

Zudem ist unklar, ob eine abstrakte Eignung der Straftat ihrer Art nach genügt oder eine konkrete Eignung im Einzelfall erforderlich sein soll.

Der Gesetzgeber nennt in seiner Begründung als Beispiele Wohnungseinbruchskriminalität, die das Sicherheitsempfinden der Bevölkerung in höchstem Maße beeinträchtigen könne und bezieht sich dabei auf die erhöhte Strafandrohung in § 244 Abs. 1 Nr. 3, Abs. 4 StGB. Daneben nennt der

Gesetzgeber aber auch organisierte Betrugsdelikte und nimmt ohne weitere Begründung an, dass diese den Rechtsfrieden ungemein störten,

> LT-Drs. 19/1557, S. 27.

Dabei sind die Aufzählungen jedoch nicht abschließend, sodass trennscharfe Grenzen für das Tatbestandsmerkmal auch nicht aus der Gesetzesbegründung gefolgert werden können. Die Organisiertheit der Tatbegehung allein kann für eine Annahme, dass eine drohende Straftat geeignet sei, den Rechtsfrieden erheblich zu beeinträchtigen, jedenfalls nicht herangezogen werden. Daher fehlt es sowohl für die normanwendende Verwaltung als auch für die Justiz an zureichenden Kriterien, die die Bestimmung der Anforderungen an die Eignung zur Störung des Rechtsfriedens ermöglichen können.

Jedenfalls für Bürger*innen sind die Grenzen aufgrund der mehrfach weichzeichnenden Begriffe der Eignung, des Rechtsfriedens und der erheblichen Weise nicht nachvollziehbar.

Die bayerische Polizei setzt die Analysesoftware „VeRA“ auf Grundlage von Art. 61a Abs. 2 Satz 1 Nr. 2 BayPAG dennoch vielfach auch zum Schutz von Eigentums- und Vermögenswerten ein,

> Anfragen zum Plenum (zur Plenarsitzung am 21. Mai 2025) mit den dazu eingegangenen Antworten der Staatsregierung, LT-Drs. 19/6865, S. 2 f.; Präsidentin des Bayerischen Landtags, Antwort auf die schriftliche Anfrage des Abgeordneten Benjamin Adjei vom 28.04.2025 betreffend Einsatz und Betrieb der polizeilichen Analyseplattform VeRA, **Anlage 13**, S. 2 ff.

(b) Art. 61a Abs. 1 Satz 1 Nr. 2 lit. d) BayPAG

Die in Art. 61a Abs. 2 Satz 1 Nr. 2 lit. d) BayPAG vorgesehenen Kulturgüter von mindestens überregionalem Rang genügen nicht den Anforderungen an Bestimmtheit und Normenklarheit. Selbst bei einer bestimmtheitskonformen Begrenzung der Rechtsgüter stellen Kulturgüter von mindestens überregionalem Rang im Sinne des Gesetzes keine besonders gewichtigen Rechtsgüter dar.

Die Anknüpfung an Kulturgüter von mindestens überregionalem Rang ist nicht hinreichend bestimmt und normenklar. In der Norm selbst und der Gesetzesbegründung fehlt es an weiteren Auslegungskriterien,

> LT-Drs. 19/1557, S. 26.

Nach dem Wortlaut ist schon nicht ausgeschlossen, dass von dem Begriff der Kulturgüter auch andere Rechtsgüter als Sachwerte umfasst sind. Nach Duden ist Kulturgut „etwas, was als kultureller Wert Bestand hat und bewahrt wird“,

> „Kulturgut, das“, https://www.duden.de/rechtschreibung/Kulturgut.

Auch eine Eingrenzung auf bestimmte Arten von Kulturgütern ist dem Wortlaut selbst nicht zu entnehmen. Der Norm ist insbesondere nicht zu entnehmen, ob der Schutz auf materielle Kulturgüter wie Bauwerke und Kunstwerke beschränkt oder auch verhaltensbezogene, nicht materielle Kulturgüter wie Feste oder traditionsreiche Veranstaltungen umfasst sein sollen.

Zieht man zur Auslegung des Begriffes die nicht explizit in Bezug genommene Gesetzesbegründung zur Einführung des Begriffs im Rahmen von Art. 11a Abs. 2 Nr. 4 BayPAG heran, wären unter dem Begriff

> „in Anlehnung an § 2 Abs. 1 Nr. 10 Kulturgutschutzgesetz jede bewegliche Sache oder Sachgesamtheit von künstlerischem, geschichtlichem oder archäologischem Wert oder aus anderen Bereichen des kulturellen Erbes, insbesondere von paläontologischem, ethnographischem, numismatischem oder wissenschaftlichem Wert zu verstehen",
>
> LT-Drs. 18/13718, S. 24.

Nach dieser Definition wären Kulturgüter auf bewegliche Sachen und Sachgesamtheiten beschränkt, unbewegliche Sachen wie Baudenkmäler wären ausgeschlossen

Diese Beschränkung zieht der Bayerische Verfassungsgerichtshof, nachdem er sich zur Auslegung des Begriffs des Kulturgutes im Rahmen von

Art. 11a Abs. 2 Nr. 4 BayPAG auf das Kulturschutzgesetz bezieht, in Zweifel, da diese im Gesetzeswortlaut nicht angelegt sei,

> BayVerfGH, Entscheidung vom 13. März 2025, 5-VIII-18, Vf. 7-VII-18, Vf. 10-VIII-18, Vf. 16-VIII-18, Rn. 150.

Damit ist schon im ersten Schritt der Auslegung unklar, ob nur bewegliche oder auch unbewegliche Sachen oder ob auch andere Rechtsgüter als bewegliche und unbewegliche Sachen umfasst sind. Schon dies ist mit den Grundsätzen der Bestimmtheit und Normenklarheit nicht vereinbar.

Aber auch der notwendige Wert von Kulturgütern als Rechtsgüter ist zudem jedenfalls teilweise ideell und verfassungsrechtlich schwer quantifizierbar. Der Wert als Kulturgut ist subjektiv und gesellschaftlich wertend. Ob ein Gegenstand einen kulturellen Wert aufweist oder kulturelles Erbe darstellt, ist nicht vollständig objektiv und an Fakten feststellbar und kann von unterschiedlichen Menschen sehr unterschiedlich beurteilt werden. So kann beispielsweise ein besonderes, auffälliges Gebäude oder Denkmal entweder als kultureller Wert oder als störend und unpassend empfunden werden.

Ebenso wenig bestimmt ist das Kriterium des mindestens überregionalen Rangs. Überregional kann sich sowohl auf soziokulturelle Regionen wie auf verwaltungsorganisatorische Untergliederungen (Landkreise, Regierungsbezirke) beziehen. Dabei ist nicht klar, ob mit überregional dann bereits ein landesweiter oder sogar ein die Landesgrenzen überschreitender Rang erforderlich ist oder ob auch ein Rang nur in Teilen eines Bundeslandes genügen soll.

Sowohl die Einstufung als Kulturgut als auch die Bestimmung eines mindestens überregionalen Rangs lassen keine ausreichenden Grenzen zur Rechtfertigung der vorgesehenen Datenanalysen als schwerwiegenden Grundrechtseingriffe erkennen. Die genannten Rechtsgüter sind sowohl in der gegenständlichen Reichweite, in der Bestimmung des kulturellen Werts und mangels klarer Kriterien und Festlegung des „überregionalen Rangs“ für normanwendende Polizist*innen und Gerichte konturlos und auch im Wege der Auslegung nicht ausreichend einschränkbar,

a.A. BayVerfGH, Entscheidung vom 13. März 2025, 5-VIII-18, Vf. 7-VII-18, Vf. 10-VIII-18, Vf. 16-VIII-18, Rn. 150.

Jedenfalls sind diese Begriffe auch für potenziell Betroffene der Datenanalysen nicht derart normenklar, dass diese Personen sichere Schlüsse auf die Anwendbarkeit der Norm ziehen könnten. Dies gilt insbesondere für die Bestimmung des mindestens überregionalen Rangs, der für Bürger*innen ohne weitere Kriterien uneindeutig verbleibt. Sogar, wenn für diese die Eigenschaft als Kulturgut im Einzelfall feststünde, ist eine trennscharfe Einordnung, ob dieses von überregionalem Rang ist, für alle gerade nicht national bedeutsamen Kulturgüter kaum möglich.

Selbst bei Heranziehung der oben genannten Eingrenzungen handelt es sich bei Kulturgütern von mindestens überregionalem Rang jedenfalls nicht um überragend wichtige Rechtsgüter, sondern um bloße Sachwerte, die schon der Normsystematik entsprechend über die abschließend als besonders gewichtige Rechtsgüter anerkannten Anlagen in Art. 61a Abs. 1 Satz 1 Nr. 3 BayPAG hinausgehen.

Auch im Vergleich zu den anderen in Art. 61a Abs. 2 Satz 1 Nr. 2 BayPAG genannten Rechtsgütern bleiben diese in Gewicht und Bedeutung zurück,

ebenfalls zweifelnd *Benamor*, BayVBl 2025, 44 (47).

Das gilt schon deshalb, weil ein kultureller Wert nicht in gleicher Weise unmittelbar an überragend wichtige Rechtsgüter wie Leben, Leib oder Bestand und Sicherheit des Bundes oder eines Landes anknüpft, wie die in Art. 61a Abs. 1 Satz 1 Nr. 3 BayPAG genannten Anlagen der kritischen Infrastruktur oder sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen. Gefahren für Kulturgütern von mindestens überregionalem Rang kommt insoweit selbst kein Rang als überragend wichtiges Rechtsgut zu.

(2) Unzureichende Eingriffsschwelle wegen drohender Gefahr

Die Eingriffsschwelle des Art. 61a Abs. 2 Satz 1 Nr. 2 BayPAG umfasst die Abwehr einer Gefahr oder einer drohenden Gefahr. Letztere genügt nicht

den verfassungsrechtlichen Anforderungen an die erforderliche konkretisierte Gefahr (siehe bereits zu Art. 61a Abs. 1 Satz 1 BayPAG unter **D.II.1.a.bb.bbb.**).

b. Hilfsweise bei reduziertem Eingriffsgewicht

Selbst wenn eine hinreichende Reduzierung des Eingriffsgewichts des Art. 61a Abs. 2 Satz 1 Nr. 1, 2 BayPAG vorgenommen worden wäre, wären die verfassungsrechtlichen Anforderungen nicht erfüllt.

Stellen automatisierte Datenanalysen keine schwerwiegenden, sondern weniger gewichtige Grundrechtseingriffe dar, können sie schon aus geringerem Anlass gerechtfertigt sein, als dies für schwerwiegende Grundrechtseingriffe erforderlich ist,

> BVerfGE 165, 363 (410 Rn. 103; 411 Rn. 107).

Während bei eingriffsintensiven Maßnahmen eine konkretisierte Gefahr und der Schutz besonders gewichtiger Rechtsgüter zusammenkommen müssen, genügt bei weniger eingriffsintensiven Maßnahmen, wenn die gesetzliche Ermächtigungsnorm eine konkretisierte Gefahr oder den Schutz besonders gewichtiger Rechtsgüter voraussetzt,

> BVerfGE 165, 363 (411 Rn. 107).

aa. Art. 61a Abs. 2 Satz 1 Nr. 1 BayPAG

Art. 61a Abs. 2 Satz 1 Nr. 1 BayPAG knüpft mit dem Verweis auf § 100b Abs. 2 StPO nicht an die Verhinderung schwerer oder besonders schwerer Straftaten an (siehe dazu **D.II.1.a.cc.aaa.(3)**). Daher müsste mindestens die Eingriffsschwelle ausreichend streng sein und eine konkretisierte Gefahr voraussetzen. Allerdings bleibt auch diese hinter den Anforderungen an eine konkretisierte Gefahr zurück (siehe dazu **D.II.1.a.cc.aaa.(1)**).

Ohne die erforderliche Voraussetzung einer konkretisierten Gefahr verbleibt der in Bezug genommene Straftatenkatalog zu weitgehend. Darüber hinaus bleibt es bei einer verfassungsrechtlichen Unzulässigkeit der dynamischen Verweisung auf § 100b Abs. 2 StPO als bundesgesetzliche Norm

(siehe dazu **D.II.1.a.cc.aaa.(2)**). Auch eine verfassungskonforme Auslegung des Art. 61a Abs. 2 Satz 1 Nr. 1 BayPAG als statische Verweisung führt mit Blick auf die zu weit gehenden geschützten Rechtsgüter nicht zu einer Verfassungskonformität der Norm.

bb. Art. 61a Abs. 2 Satz 1 Nr. 2 BayPAG

Aufgrund der in Bezug genommenen drohenden Gefahr gemäß Art. 11a Abs. 1 BayPAG genügt Art. 61a Abs. 2 Satz 1 Nr. 2 BayPAG nicht den Rechtfertigungsanforderungen auch bei geringerem Eingriffsgewicht. Die Ermächtigungsgrundlage des Art. 61a Abs. 2 Satz 1 Nr. 2 BayPAG sieht nicht nur besonders gewichtige Rechtsgüter vor, die zudem zu unbestimmt geregelt sind (siehe dazu **D.II.1.a.cc.bbb.(1)**). Gleichzeitig bleibt auch die Eingriffsschwelle hinter der erforderlichen konkretisierten Gefahr zurück (siehe dazu oben **D.II.1.a.cc.bbb.(2)** und **D.II.1.a.bb.bbb**).

c. Hilfsweise bei Ausreichen der drohenden Gefahr

Selbst wenn eine ausreichende Eingriffsschwelle auch bei Bezugnahme der drohenden Gefahr nach Art. 11a Abs. 1 BayPAG vorläge, würden die vorgesehenen Eingriffsschwellen und Schutzgüter in Art. 61a Abs. 2 Satz 1 Nr. 1, Nr. 2 BayPAG nicht den verfassungsrechtlichen Anforderungen genügen, da Art. 61a Abs. 2 BayPAG schwerwiegende Grundrechtseingriffe ermöglicht.

Art. 61a Abs. 2 Satz 1 Nr. 1 BayPAG sieht weiterhin keine konkretisierte Gefahr als Eingriffsschwelle und gleichzeitig auch nicht nur schwere und besonderes schwere Straftaten als Schutzgüter vor. Auch bleibt der dynamische Verweis auf § 100b Abs. 2 StPO verfassungswidrig.

Art. 61a Abs. 2 Satz 1 Nr. 2 BayPAG sähe bei dieser Annahme eine zureichende Eingriffsschwelle vor, knüpfte aber nach wie vor an nicht ausreichend gewichtige und unbestimmte Rechtsgüter an.

Die dargestellten Mängel (siehe **D.II.1.a.cc.aaa.**) führen dazu, dass Art. 61a Abs. 2 Satz 1 Nr. 1 BayPAG selbst bei geringerem Eingriffsgewicht und einer hinreichenden Eingriffsschwelle verfassungswidrig wäre. Ebenso wäre

Art. 61a Abs. 2 Satz 1 Nr. 2 BayPAG mangels ausreichender Bestimmtheit und Normenklarheit (siehe **D.II.1.a.cc.bbb.**) auch in diesem Falle verfassungswidrig.

2. Defizitäre datenschutzrechtliche Kontrolle hinsichtlich aller Tatbestandsvarianten

Art. 61a BayPAG sieht für keine seiner Tatbestandsvarianten (Art. 61a Abs. 1 Satz 1, Abs. 2 Satz 1 Nr. 1, 2 BayPAG) die verfassungsrechtlich gebotenen Vorkehrungen für Transparenz, individuellen Rechtsschutz und aufsichtliche Kontrolle vor.

a. Maßstab

Die Anforderungen an Transparenz, individuellen Rechtsschutz und aufsichtliche Kontrolle folgen aus dem Verhältnismäßigkeitsgrundsatz,

> BVerfGE 165, 363 (412 f. Rn. 109 m.w.N.),

und ergeben sich aus dem jeweiligen Grundrecht in Verbindung mit Art. 19 Abs. 4 GG,

> BVerfGE 141, 220 (282 Rn. 134).

Der Verhältnismäßigkeitsgrundsatz stellt für tief in die Privatsphäre reichende Überwachungsmaßnahmen deshalb an eine wirksame Ausgestaltung dieser Kontrolle sowohl auf der Ebene des Gesetzes als auch der Verwaltungspraxis gesteigerte Anforderungen,

> BVerfGE 141, 220 (284 Rn. 140).

Insbesondere einer sachgerechten Ausgestaltung der Kontrolle kommt große Bedeutung zu,

> BVerfGE 165, 363 (412 f. Rn. 109).

Diese kann angesichts der möglicherweise hohen Zahl von Maßnahmen etwa nach einem abgestuften Kontrollkonzept zwischen unabhängigen und behördlichen Datenschutzbeauftragten aufgeteilt und auch als stichprobenartiges Vorgehen geregelt werden,

BVerfGE 165, 363 (412 f. Rn. 109).

Dabei kompensieren aufsichtliche Kontrollen durch mit wirksamen Befugnissen ausgestatteten Stellen den schwach ausgestalteten Individualrechtsschutz bei heimlichen Überwachungsmaßnahmen. Von besonderer Bedeutung ist daher ihre regelmäßige Durchführung in angemessenen Abständen von maximal etwa zwei Jahren,

BVerfGE 141, 220 (285 Rn. 141).

b. Kein ausreichendes Kontrollkonzept in Art. 61a BayPAG

Art. 61a PAG selbst enthält keine Regelungen zur datenschutzrechtlichen Kontrolle, sondern ordnet nur vorbereitende bzw. begleitende Maßnahmen an.

Nach Art. 61a Abs. 4 Satz 4 BayPAG muss das Vorliegen der tatbestandlichen Voraussetzungen der Art. 61a Abs. 1, 2 BayPAG dokumentiert werden. Dazu bedarf es nach Gesetzesbegründung einer „eigenständig ausformulierten Begründung“,

vgl. LT-Drs. 19/1557, S. 29.

Darüber hinaus ist das Vorgehen bei Maßnahmen nach Art. 61a Abs. 1, 2 BayPAG gemäß Art. 61a Abs. 4 Satz 5 BayPAG zu protokollieren.

Die Entwurfsbegründung spricht hierbei (noch zu Satz 4 in der Entwurfsfassung) von einer ausführlichen Protokollierung der Verarbeitungsvorgänge, um eine Kontrolle der Rechtmäßigkeit und eine Eigenüberwachung der durchgeführten Maßnahmen zu ermöglichen. Deren inhaltliche Anforderung richte sich nach den allgemeinen datenschutzrechtlichen Bestimmungen des BayPAG nach Art. 63 Abs. 2 BayPAG,

vgl. LT-Drs. 19/1557, S. 29.

Damit müssen nach Art. 63 Abs. 2 Satz 1 BayPAG Erhebung, Veränderung, Abruf, Offenlegung einschließlich Übermittlung, Verknüpfung und Löschung protokolliert werden. Protokolle über Abrufe und Offenlegungen müssen nach Art. 63 Abs. 2 Satz 2 BayPAG die dafür maßgeblichen Gründe

nennen sowie Datum und Uhrzeit dieser Vorgänge enthalten und, soweit möglich, die Feststellung der Identität der abrufenden oder offenlegenden Person sowie des Empfängers ermöglichen.

Weitergehende Vorgaben sieht Art. 61a BayPAG jedoch nicht vor. Insbesondere sind keine Verweisungen auf andere gesetzliche Kontrollmechanismen im Normtext enthalten.

c. Keine Sicherungen in anderen Bestimmungen des geltenden Rechts

Der Gesetzgeber beruft sich in der Begründung auf die Errichtungsanordnung und Datenschutzfolgenabschätzung gemäß Art. 64 BayPAG als externe datenschutzrechtliche Kontrolle durch eine unabhängige Instanz,

> vgl. LT-Drs. 19/1557, S. 26.

Gemäß Art. 64 Abs. 1 Satz 2 und Satz 3 BayPAG sind dem*der Landesbeauftragten für den Datenschutz die Errichtungsanordnung und wesentliche Änderungen des Verfahrens mitzuteilen. Nach Art. 64 Abs. 2 Satz 1 BayPAG muss die Polizei vor der erstmaligen Anwendung einer Datenverarbeitung eine Folgenabschätzung für den Schutz personenbezogener Daten durchführen, wenn eine Datenverarbeitung oder deren Änderung aufgrund ihrer Art, ihres Umfangs, ihres Zwecks, des Einsatzes neuer Technologien oder sonstiger Umstände voraussichtlich ein hohes Risiko für die Rechte natürlicher Personen birgt. Gemäß Art. 64 Abs. 2 Satz 6 BayPAG hat der*die Landesbeauftragte vor der erstmaligen Anwendung jedoch lediglich Gelegenheit zur Stellungnahme, wozu ihm*ihr auf Anforderung alle für seine*ihre Kontrolle erforderlichen und für die Polizei verfügbaren Informationen zu übermitteln sind (Art. 64 Abs. 2 Satz 8 BayPAG).

Gemäß Art. 64 Abs. 3 Satz BayPAG ist lediglich die speichernde Stelle, mithin die Polizei selbst, verpflichtet, in angemessenem Abstand die Notwendigkeit der Weiterführung oder Änderung ihrer Daten zu prüfen.

Weitergehende besondere Kontrollbefugnisse des*der Landesbeauftragten für den Datenschutz bestehen nicht. Insbesondere findet Art. 51 Abs. 2

Satz 1 BayPAG keine Anwendung, da dieser ausdrücklich nur für Maßnahmen gemäß der Art. 34 bis 46 BayPAG gilt und auch systematisch im „2. Unterabschnitt Besondere Befugnisse und Maßnahmen der Datenerhebung“ normiert ist. Art. 61a BayPAG steht demgegenüber im 3. Unterabschnitt „Datenspeicherung, -übermittlung und sonstige Datenverarbeitung“. Eine Bezugnahme des Art. 51 BayPAG erfolgt in Art. 61a BayPAG gerade nicht. Der Gesetzgeber geht vielmehr davon aus, dass Kontrollpflichten bereits im Rahmen der Datenerhebung Anwendung fänden,

> vgl. LT-Drs. 19/1557, S. 29,

und folgert daraus unzutreffend, dass eine weitere Kontrolle der Maßnahmen nach Art. 61a BayPAG selbst damit nicht mehr erforderlich sei.

Im Übrigen bleibt es bei den allgemeinen Befugnissen des*der Landesbeauftragten für den Datenschutz, wenngleich diese nicht explizit in Bezug genommen werden. Diese ergeben sich aus Art. 16 des BayDSG. Nach diesem hat der*die Landesbeauftragte für den Datenschutz Auskunftsrechte und ein Recht auf Unterlagenvorlage sowie Betretungsrechte (Art. 16 Abs. 1 Satz 2, 3 BayDSG). Verpflichtungen zu Kontrollen oder eine Regelmäßigkeit von Kontrollen sind gesetzlich nicht vorgesehen.

Eine vorgesehene Selbstkontrolle gemäß Art. 64 Abs. 3 BayPAG genügt nicht den Anforderungen an unabhängige und externe Kontrollen.

Eine Errichtungsanordnung und Datenschutzfolgenabschätzung nach Art. 64 BayPAG und die allgemeinen Befugnisse für die datenschutzrechtliche Kontrolle sind aber keinesfalls ausreichend, um den verfassungsrechtlichen Anforderungen gerecht zu werden. Kontrollbefugnisse oder -pflichten sind damit nicht verbunden. Das vorgesehene Konzept ist daher aus verfassungsrechtlicher Sicht nicht genügend, um die Verhältnismäßigkeit der schwerwiegenden Grundrechtseingriffe sicherzustellen,

> so auch zu dem Gesetzentwurf, der, bis auf kleinste Änderungen, der nun geltenden Regelung entspricht *Petri*, Stellungnahme zum Fragenkatalog im Rahmen der Anhörung des Ausschusses für Kommu-

> nale Fragen, Innere Sicherheit und Sport zum Gesetzentwurf zur Änderung des Polizeiaufgabengesetzes und weiterer Rechtsvorschriften am 16. Mai 2024 – **Anlage 11**, S. 18.

Es ist bereits für eine aufsichtliche Kontrolle im Zeitpunkt der Errichtung einer Datenanalyseplattform unzureichend, wenn an die externe Kontrollinstanz nur eine Mitteilung erfolgt und diese lediglich Gelegenheit zur Stellungnahme erhält. Schon in diesem erstmaligen Zeitpunkt sind keine tatsächlichen Kontrollmöglichkeiten bzw. -verpflichtungen vorgesehen,

> zu dem Gesetzentwurf, der, bis auf kleinste Änderungen, der nun geltenden Regelung entspricht *Petri*, Stellungnahme zum Fragenkatalog im Rahmen der Anhörung des Ausschusses für Kommunale Fragen, Innere Sicherheit und Sport zum Gesetzentwurf zur Änderung des Polizeiaufgabengesetzes und weiterer Rechtsvorschriften am 16. Mai 2024 – **Anlage 11**, S. 18.

Die Datenschutzfolgeabschätzung nach Art. 64 Abs. 2 Satz 1 BayPAG verfolgt nur eine präventive Zielrichtung vor Inbetriebnahme und kann eine Kontrolle nicht ersetzen. Dies gilt umso mehr, da die geplante Software bereits im Einsatz ist.

Ebenso wenig ist sichergestellt, dass eine Stellungnahme, die Bedenken bezüglich der Verfassungsgemäßheit bzw. Rechtmäßigkeit der vorgesehenen Datenanalyse anbringt, tatsächlich Beachtung findet und Änderungen nach sich zieht bzw. Auswirkungen auf die Errichtung hat,

> zu dem Gesetzentwurf, der, bis auf kleinste Änderungen, der nun geltenden Regelung entspricht *Petri*, Stellungnahme zum Fragenkatalog im Rahmen der Anhörung des Ausschusses für Kommunale Fragen, Innere Sicherheit und Sport zum Gesetzentwurf zur Änderung des Polizeiaufgabengesetzes und weiterer Rechtsvorschriften am 16. Mai 2024 – **Anlage 11**, S. 18.

Darüber hinaus ist aber eine Kontrolle nur im Zeitpunkt der Errichtung der Analyseplattform unzureichend, um den verfassungsrechtlichen Anforderungen an wirksame und verhältnismäßigkeitssichernde Kontrollen zu ge-

nügen. Angesichts der Kompensationsfunktion der aufsichtlichen Kontrolle für den schwach ausgestalteten Individualrechtsschutz kommt gerade der regelmäßigen Durchführung im eigentlichen Analysebetrieb besondere Bedeutung zu,

BVerfGE 141, 220 (285 Rn. 141).

Nur auf diesem Wege kann sichergestellt werden, dass Fehler des Systems, aber auch Missbrauch der Plattform erkannt und verhindert werden können.

Da vorliegend im Rahmen des Analysebetriebes keinerlei regelmäßige Kontrollen vorgesehen sind, ist deren Durchführung nicht gewährleistet. Daher stellen sich Fragen zur verfassungskonformen Ausgestaltung des „wie“ des Kontrollkonzeptes vorliegend nicht. Es fehlt bereits am „ob“ einer regelmäßigen unabhängigen Kontrolle nach Einrichtung des Analysesystems.

Auch weitere allgemeine Regelungen insbesondere des BayDSGs führen nicht zu einer anderen Bewertung des fehlenden Kontrollkonzeptes. Gemäß Art. 66 BayPAG findet das BayDSG lediglich ergänzend Anwendung, soweit das BayPAG keine spezielleren Regelungen enthält. Die darüber anwendbaren allgemeinen Vorschriften des bayerischen Datenschutzgesetzes stellen kein ausreichendes Kontrollniveau sicher.

Insbesondere die Vorgaben in Art. 5 Abs. 3 Satz 1 BayDSG zur Prüfung und Wartung automatisierter Verfahren und Datenverarbeitungsanlagen durch den Verweis auf Art. 28 Abs. 1-4, 9, 10 DSGVO enthalten nur Vorgaben zur Ausgestaltung bei der Arbeit mit anderen Auftragsverarbeiter*innen und keine Vorgaben zur externen Kontrolle. Ebenso wenig sieht Art. 7 BayDSG Kontrollkonzepte vor, sondern regelt lediglich allgemeine Vorgaben zur Zulässigkeit automatisierter Verfahren. Art. 32 BayDSG verpflichtet im Falle automatisierter Datenverarbeitung Verantwortliche und Auftragsverarbeiter*innen, auf Grundlage einer Risikobewertung Maßnahmen auch zur Sicherung der Daten u.a. vor unbefugtem Zugriff (Abs. 2 Nr. 1, 3 lit. a) sowie Missbrauch und unbefugter Nutzung sowie zum Schutz bei Übermittlung (Abs. 2 Nr. 3 lit. b)-d)). Die Norm selbst enthält jedoch

keine konkreten Vorgaben zu einem tatsächlichen Kontrollkonzept, das den Anforderungen des angerufenen Gerichts genügt, insbesondere keine regelmäßigen Kontrollen des Analysebetriebs. Eine unabhängige und wirksame Kontrolle wird daher gerade nicht sichergestellt. Meldepflichten nach Art. 33 BayDSG, welcher auf Art. 33 Abs. 3 DSGVO verweist, stellen auch keine hinreichende Sicherung dar, da sie ein aktives Tätigwerden des Verantwortlichen voraussetzen und lediglich Einzelfälle betreffen.

Die aufgrund von Art. 61a BayPAG eingesetzte Software „VeRA“ wurde 2023 zwar vom Fraunhofer Institut geprüft, dabei wurden keine Funktionalitäten festgestellt, die einen unzulässigen Datenabfluss unter Umgehung von Zugriffsbeschränkungen oder unautorisierten Zugriff ermöglichen,

> vgl. Süddeutsche Zeitung, Bayerische Polizei darf umstrittene Analyse-Software von Palantir nutzen, 8. März 2023, https://www.sueddeutsche.de/bayern/bayern-analyse-software-polizei-fraunhofer-institut-1.5765122.

Die Erforderlichkeit dieser Prüfung für den Softwareeinsatz ist jedoch bereits nicht verpflichtend im Gesetz vorgesehen und kann schon aus diesem Grunde keine Auswirkungen auf das mangelnde datenschutzrechtliche Kontrollkonzept haben. Das Gutachten des Instituts ist zudem nicht öffentlich zugänglich, sodass unklar verbleibt, in welchem Umfang eine Prüfung tatsächlich erfolgt ist. Zudem erfolgte die Kontrolle einmalig basierend auf dem damaligen Stand der Software, sodass Updates der Software keiner Prüfung mehr unterzogen werden,

> vgl. *Reuter*, Nicht eingesetzte Polizei-Software kostet Millionen, 10. März 2023, https://netzpolitik.org/2023/palantir-in-bayern-nicht-eingesetzte-polizei-software-kostet-millionen/.

Weitere externe Kontrollen der Software sind nicht bekannt.

d. Keine Vorkehrungen gegen Fehleranfälligkeit

Obwohl Art. 61a BayPAG den Einsatz komplexer Methoden ermöglicht (siehe oben unter **D.I.2.a.bb.**), hat der Gesetzgeber keine flankierenden Schutzmaßnahmen getroffen,

> so auch zu dem Gesetzentwurf, der, bis auf kleinste Änderungen, der nun geltenden Regelung entspricht *Zöller*, Schriftliche Stellungnahme zum Gesetzentwurf der Staatsregierung für ein Gesetz zur Änderung des Polizeiaufgabengesetzes und weiterer Rechtsvorschriften vom 9. April 2024 (LT-Drs. 19/1557) – **Anlage 12**, S. 15.

Das angerufene Gericht fordert aber bei komplexeren Formen des automatisierten Abgleichs von Daten, dass Vorkehrungen gegen eine hiermit spezifisch verbundene Fehleranfälligkeit getroffen werden, was auch gesetzliche Regelungen zu einem staatlichen Monitoring der Entwicklung der eingesetzten Software erfordern kann,

> BVerfGE 165, 363 (412 Rn. 109).

Gerade weil für die Ausführung der Analysen im Sinne des Art. 61a BayPAG auf das System eines privaten Anbieters zurückgegriffen wird, sind gesetzliche Regelungen zur Erkennung und Vermeidung von Fehlern erforderlich,

> Bedenken zu den „verfassungsrechtlichen Anforderungen nach einer ausreichenden Datenqualität“ schon mit Blick auf die Ausgangsdaten zu dem Gesetzentwurf, der, bis auf kleinste Änderungen, der nun geltenden Regelung entspricht *Petri*, Stellungnahme zum Fragenkatalog im Rahmen der Anhörung des Ausschusses für Kommunale Fragen, Innere Sicherheit und Sport zum Gesetzentwurf zur Änderung des Polizeiaufgabengesetzes und weiterer Rechtsvorschriften am 16. Mai 2024 – **Anlage 11**, S. 17.

Solche gesetzlichen Vorgaben lassen sich weder dem BayPAG noch dem über Art. 66 BayPAG ergänzend anwendbaren BayDSG entnehmen.

Art. 48 Abs. 7 BayPAG sieht vor, dass personenbezogene Daten, die durch die in den Abs. 1 und 4 bezeichneten Maßnahmen erhoben wurden, ent-

sprechend dem Stand der Technik gegen unbefugte Kenntnisnahme, Veränderung und Löschung besonders zu sichern sind. Die Norm findet jedoch bereits keine Anwendung auf Analysen nach Art. 61a BayPAG, da sie, anders als Art. 48 Abs. 1, 3 und 4, Art. 53 Abs. 2 und Art. 54 Abs. 2 BayPAG, in Art. 61a Abs. 1 Satz 3 BayPAG nicht in Bezug genommen wird. Zudem ist Sinn und Zweck der Norm, die erhobenen Daten gegen die Einflussnahme unbefugter Dritter zu schützen. Die Fehleranfälligkeit, die sich aus dem Einsatz einer komplexen Methode selbst ergibt, wird durch die Vorschrift nicht vermindert.

Art. 53 Abs. 5 Satz 2 BayPAG schreibt Prüfungstermine vor, an denen bei automatisierten Dateien die Erforderlichkeit der Speicherung zu überprüfen ist. Auch diese Norm findet mangels Bezugnahme bereits keine Anwendung auf Art. 61a BayPAG. Die Pflicht zur Prüfung der Erforderlichkeit einer Speicherung von Daten selbst umfasst auch keine Prüfung hinsichtlich der Richtigkeit der Daten, bzw. Abgleichschritte und -ergebnisse bei und nach dem Einsatz einer Analyse nach Art. 61a BayPAG.

Gemäß Art. 54 Abs. 5 BayPAG soll die Polizei angemessene Maßnahmen ergreifen, dass gespeicherte personenbezogene Daten sachlich richtig, vollständig und erforderlichenfalls auf dem neusten Stand sind, und zu diesem Zweck die Qualität der Daten überprüfen. Auch diese Norm findet mangels Bezugnahme keine Anwendung. Die Vorschrift dient der Umsetzung des Art. 4 Abs. 1 lit. d) JI-Richtlinie und bezieht sich nur auf Richtigkeit, Vollständigkeit und Aktualität der gespeicherten personenbezogenen Daten selbst. Vorgaben zu Maßnahmen, die die Funktionsfähigkeit, Aktualität und Fehlerfreiheit der Analysesoftware (bzw. der technischen Mittel) und die Richtigkeit und Vollständigkeit von Abgleich- bzw. Analyseergebnissen sicherstellen, enthält Art. 54 Abs. 5 BayPAG aber nicht. Sie stellt also keine Vorschrift dar, die sich auf die Fehleranfälligkeit bezieht, die sich aus dem Einsatz eines komplexen Systems gemäß Art. 61a BayPAG ergibt.

Art. 62 Abs. 1 Satz 1 BayPAG schreibt vor, dass personenbezogene Daten zu berichtigen sind, wenn sie unrichtig sind. Satz 2 sieht vor, dass die Berichtigung auch eine Ergänzung der Daten erforderlich machen kann, wenn

eine mangelnde Vollständigkeit die Unrichtigkeit der Daten für den Verarbeitungszweck zur Folge hat.

Auch diese Vorschrift bezieht sich auf die personenbezogenen Daten selbst. Sie enthält keine Vorgaben für die Überprüfung der Funktionsweise und Ergebnisse der automatisierten Datenanalyse. Fehler, die Ergebnis einer fehlerhaften Analyse und nicht von unrichtigen personenbezogenen Daten selbst sind, sind nicht erfasst. Auch eine Ergänzung der unvollständigen personenbezogenen Daten nach Satz 2 erweitert die Berichtigungspflicht nicht auf Vorgang und Ergebnis von Datenanalysen nach Art. 61a BayPAG.

Art. 32 Abs. 2 Nr. 4 lit. e) BayDSG schreibt für den Fall der automatisierten Verarbeitung vor, dass auf Grundlage einer Risikobewertung Maßnahmen zu ergreifen sind, die geeignet sind, um zu gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit). Die Norm verpflichtet bei automatisierten Datenverarbeitungen, wie sie auch im Rahmen von Art. 61a BayPAG erfolgen, jedoch nur dazu, sicherzustellen, dass die Verarbeitung durchgeführt werden kann und neu auftretende Fehlfunktionen durch Meldung erkannt und korrigiert werden können. Sie enthält damit keine ausreichenden Vorgaben dazu, wie Fehler bereits vor bzw. bei Inbetriebnahme der technischen Mittel zur Datenverarbeitung ausgeschlossen bzw. weniger wahrscheinlich gemacht werden können.

Zudem setzt die Meldung auftretender Fehlfunktionen voraus, dass der Fehler für Anwender*innen erkennbar ist. Die Fehleranfälligkeit, die im Zusammenhang mit dem Einsatz komplexer Systeme steht, wird hierdurch nicht adressiert. Denn ein Fehler, der nur bei Betrachtung der Software selbst und nicht des Outputs erkennbar ist, wird durch die Vorschrift nicht geregelt. Die Norm adressiert das hohe Fehlerpotenzial beim Einsatz hochkomplexer Analysesoftware wie der in Bayern eingesetzten auf Palantir Gotham basierenden Software „VeRA“ damit nur unzureichend.

Für dieses Risiko bedarf es gerade klarer gesetzgeberischer Vorgaben an die ausführende Verwaltung, wie die Funktionsfähigkeit und vor allem

Fehlerfreiheit auch vor Beginn des Einsatzes der automatisierten Verarbeitungsmittel sichergestellt wird. Die allgemeine Gewährleistungsverpflichtung des Art. 32 Abs. 4 Nr. 2 lit. e) BayDSG genügt vor dem Hintergrund der hohen Eingriffsintensität der Datenanalysen nach Art. 61a BayPAG den verfassungsrechtlichen Anforderungen an Vorgaben zur Vermeidung von Fehlern nicht.

Dies hat der Gesetzgeber für andere Verpflichtungen des Art. 32 Abs. 2 Nr. 4 BayDSG auch erkannt, indem er beispielsweise zur Wahrung von Nr. 4 lit. a) Zugriffsbeschränkungen (Art. 61a Abs. 4 Satz 1, 2 BayPAG) vorgesehen hat. Ebenso hat er durch Art. 61a Abs. 4 Satz 4 und 5 BayPAG konkretere Regelungen zur Eingabekontrolle gemäß Art. 32 Abs. 2 Nr. 4 lit. c) BayDSG getroffen. Eben solche speziellen Regelungen hätte der Gesetzgeber auch zur Vermeidung der Risiken vorsehen müssen, die sich gerade aus der Fehleranfälligkeit der Datenanalyse selbst ergeben.

Rechtsanwalt Dr. Bijan Moini

Anlagenverzeichnis