



Der Bayerische Landesbeauftragte für den Datenschutz

Bayer. Datenschutzbeauftragter • PF 22 12 19 • 80502 München

An den
Vorsitzenden des Ausschusses
für Kommunale Fragen, Innere Sicherheit und Sport

Ihr Zeichen, Ihre Nachricht vom
18.04.2024

Unser Zeichen
DSB/2-622/2-318-3

München, den 08.05.2024
Durchwahl: 089 212672 - 0

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

Sehr geehrter Herr Vorsitzender,

ich danke Ihnen für die Einladung als Sachverständiger zur Anhörung des Innenausschusses am 16. Mai 2024, der ich gerne nachkommen werde.

Zu den datenschutzrechtlichen Aspekten des übersandten Fragenkatalogs möchte ich wie folgt Stellung nehmen:

1. Art. 16 PAG-E:

Frage:

- a) *Wie beurteilen Sie die Herabsenkung der Eingriffsschwelle hinsichtlich der konkreten Gefahr für Meldeauflagen für die Polizei?*

Antwort:

Der Entwurf knüpft die Meldeanordnung nicht mehr an die Bedrohung eines bedeutenden Rechtsgutes. Diese Herabsenkung der Anforderungen für eine Meldeanordnung ist für mich nicht nachvollziehbar und die diesbezüglichen Änderungen sind aus datenschutzrechtlicher Sicht kritisch zu betrachten.

Zunächst stellt sich für mich die Frage, ob es überhaupt einen praktischen Bedarf für diese Herabsenkung der Eingriffsschwelle gibt. In der Gesetzesbegründung wird angeführt, die Hauptanwendungsfälle einer Meldeanordnung seien Maßnahmen gegen Hooligans bei Fußballspielen oder Fälle häuslicher Gewalt. In diesen Situationen dürfte regelmäßig auch das bedeutende Rechtsgut „Gesundheit“ betroffen sein, so dass ein polizeiliches Bedürfnis für den Verzicht auf diese Eingriffsschwelle nicht erkennbar ist. Darüber hinaus wird in der Begründung nur angeführt, dass derartige Maßnahmen auch bei Großveranstaltungen „denkbar“ seien, um ständige und fortgesetzte Störungen des Veranstaltungsverlaufs bzw. des Straßenverkehrs zu verhindern. Diese sehr allgemein gehaltenen Ausführungen können für mich die fachliche Notwendigkeit für eine Herabsetzung der Voraussetzungen für eine polizeiliche Meldeauflage nicht überzeugend darlegen.

Stattdessen ist zu befürchten, dass hierdurch die Zahl der polizeilichen Meldeauflagen deutlich steigen wird. Aufgrund der im Raum stehenden Streubreite ist dies ein Aspekt, den der Gesetzgeber berücksichtigen sollte. Zwar mag die Meldeauflage gegenüber einem Aufenthaltsgebot oder gar einer Ingewahrsamnahme ein milderes Mittel darstellen. Einer Person aufzuerlegen, in bestimmten zeitlichen Abständen bei einer Polizeidienststelle persönlich zu erscheinen, ist nichtsdestotrotz ein erheblicher Grundrechtseingriff, der auch das Recht auf informationelle Selbstbestimmung berührt und auf eng begrenzte Fälle beschränkt bleiben sollte.

Trotz dieser Eingriffstiefe sieht der Entwurf für die Meldeanordnung keine ausreichenden grundrechtssichernden Begleitmaßnahmen vor. Problematisch ist vor allem, dass es, da die Maßnahme jeweils um einen Monat verlängert werden kann, keine gesetzlich vorgesehene Höchstfrist gibt, die zeitlichen Abstände der Meldung nicht geregelt sind und die Anordnung letztlich durch jede Polizistin bzw. jeden Polizisten erfolgen kann.

Frage:

- b) *Ergeben sich dadurch Änderungen für die Voraussetzungen der Eingriffsschwelle der drohenden Gefahr?*

Antwort:

Grundsätzlich gibt Art. 16 PAG-E keinen Anlass, die Eingriffsschwelle der drohenden Gefahr zu verändern. Allerdings sollte der Begriff der „drohenden Gefahr“ meines Erachtens generell verfassungskonform restriktiv ausgelegt werden.

Im Kern verlangt das Tatbestandsmerkmal der drohenden Gefahr einzelfallbezogen, dass in absehbarer Zeit Angriffe von erheblicher Intensität oder Auswirkung auf bedeutende Rechtsgüter zu erwarten sind.

Anknüpfungspunkt für eine verfassungskonform restriktive Auslegung könnte dabei das in Art. 11a Abs. 1 PAG enthaltene Tatbestandsmerkmal des „Angriffs von erheblicher Intensität oder Auswirkung“ sein. Ein Angriff setzt rein begrifflich ein absichtliches, aggressives Verhalten des Angreifenden voraus, das bedeutende Rechtsgüter bedroht. Durch dieses enge Verständnis gewinnt die Legaldefinition der drohenden Gefahr eine Bedeutung, die auch begrenzende Auswirkungen auf die Legaldefinitionen der bedeutenden Rechtsgüter haben kann.

An dieser Stelle möchte ich allerdings auch darauf hinweisen, dass das Bundesverfassungsgericht seine bisherigen Feststellungen zur grundrechtlichen Einordnung der „drohenden Gefahr“ bislang nur vor dem Hintergrund der Beurteilung von polizeilichen Datenverarbeitungsprozessen getroffen hat. Der bayerische Gesetzgeber erstreckt die Wahrscheinlichkeitsschwelle der drohenden Gefahr – wie im vorliegenden Fall – jedoch auch auf polizeiliche Standard-Vollzugsmaßnahmen. Derartige Maßnahmen unterliegen in tatsächlicher Hinsicht grundlegend anderen Voraussetzungen als die in den Art. 30 ff. PAG geregelten Datenverarbeitungsprozesse. Die Verankerungen des Begriffs der drohenden Gefahr in der polizeilichen Generalklausel – ohne eine Begrenzung auf verdeckte Maßnahmen und den Schutz überragend wichtiger Rechtsgüter – führt letztlich dazu, dass die Polizei auch vermehrt im „Gefahrenvorfeld“ tätig werden kann.

Die tatsächlichen Auswirkungen lassen sich in Bezug auf polizeiliche Standardmaßnahmen nur schwer nachvollziehen, weil die Polizeikräfte insoweit nahezu generell

nicht verpflichtet sind zu dokumentieren, wenn und warum sie im Rahmen ihrer Vollzugsmaßnahmen von einer drohenden Gefahr ausgegangen sind. Eine solche Dokumentationspflicht mag bei Standardmaßnahmen des Polizeialltags dem Prinzip der effektiven Gefahrenabwehr zuwiderlaufen und schon aufgrund der schier Masse an Maßnahmen schwer zu realisieren sein. Bei der drohenden Gefahr begründet ihr Fehlen für die Betroffenen allerdings das Risiko, dass die polizeilichen Vollzugskräfte die im Vergleich zur konkreten Gefahr vermeintlich niedrigeren rechtsstaatlichen Hürden bevorzugen. Eine nachträgliche rechtsstaatliche Kontrolle wird dann bei den Vollzugsmaßnahmen nicht oder allenfalls sehr eingeschränkt erfolgen können.

2. Art. 33 Abs. 10 PAG-E

Frage:

- a) *Wie beurteilen Sie die (spezielle) Verpflichtung des Art. 33 PAG zur Übermittlung von bereits erhobenen (vorhandenen) Bildaufnahmen und -aufzeichnungen durch alle Betreiber von installierten Bildaufnahme- und -aufzeichnungsgeräten?*

Antwort:

Art. 33 Abs. 10 PAG-E soll es der Polizei erlauben, auf Bildaufnahmen und Bildaufzeichnungen anderer Betreiber von Videoüberwachungsanlagen zuzugreifen. Die in Art. 33 Abs. 10 PAG-E vorgesehenen weitreichenden Zugriffsmöglichkeiten lassen eine massive Ausdehnung der polizeilichen Nutzung von Videoüberwachungsmaterial erwarten. Unter Beachtung der Verhältnismäßigkeit und vor dem Hintergrund einer Überwachungsgesamtrechnung (vgl. BVerfGE 125, 260, 323 – Vorratsdatenspeicherung) ist die angestrebte Neuregelung daher aus datenschutzrechtlicher Sicht als bedenklich zu bewerten.

Zudem sehe ich - neben meinen Bedenken bezüglich der Gefahr einer flächendeckenden Überwachung (nähere Ausführungen unter Nummer 2.c) - hinsichtlich Art. 33 Abs. 10 PAG-E folgende grundsätzliche Probleme:

Es ist davon auszugehen, dass Datenübermittlungen auf Verlangen der Polizei gemäß Art. 33 Abs. 10 Satz 1 PAG-E regelmäßig mit einem gewissen Zeitverzug erfolgen und eine präventive Intervention daher kaum möglich sein wird. Der präventivpo-

lizeiliche Charakter dieser Regelung ist daher zweifelhaft. Sollte gespeichertes Videomaterial zu Beweis Zwecken in einem Strafverfahren benötigt werden, ist eine Sicherstellung bzw. Beschlagnahme bereits jetzt nach den Vorschriften der StPO möglich, weshalb sich mir der praktische Bedarf für die Regelung des Art. 33 Abs. 10 Satz 1 PAG-E nicht erschließt.

Art. 33 Abs. 10 PAG-E ermöglicht es der Polizei systematisiert auf Bildaufnahmen und -aufzeichnungen Dritter zuzugreifen. Die Bindung der Verwaltung an Recht und Gesetz nach Art. 20 Abs. 3 GG gebietet es, dass die Polizei in einer Konstellation wie sie der Gesetzgeber mit Art. 33 Abs. 10 PAG-E vorsieht, die Pflicht hat sicherzustellen, dass die Verarbeitung – insbesondere die Erhebung, Speicherung und zweckändernde Übermittlung – der Bildaufnahmen bzw. -aufzeichnungen durch den verpflichteten Betreiber rechtmäßig erfolgt. Eine rechtswidrige Videoüberwachung durch einen Betreiber stellt im Übrigen eine Verletzung der Rechtsordnung und damit eine Störung der öffentlichen Sicherheit dar. Sie wäre polizeilich zu unterbinden. Stattdessen erweckt Art. 33 Abs. 10 Satz 6 PAG-E den Eindruck, die Polizei müsste die Betreiber lediglich über ihre Pflichten informieren und könnte auch unrechtmäßig erhobene Bildaufnahmen und -aufzeichnungen Dritter nutzen. Im Gesetz sollte daher klar geregelt werden, dass die Polizei auf unrechtmäßig verarbeitete Daten nicht zugreifen darf.

Unabhängig davon möchte ich anmerken, dass nichtöffentliche Betreiber auch über die Vorgaben nach dem BDSG bzw. der DSGVO informiert werden müssten, da für sie das BayDSG keine Anwendung findet (s. Art. 1 BayDSG).

Frage:

- b) *Wie sehen Sie die Norm insbesondere im Hinblick auf die Aufgabe der Gefahrenabwehr und Strafverfolgung der Landespolizei auch im Bereich und im Umfang von Verkehrseinrichtungen, insbesondere in denen auch die Bundespolizei Zuständigkeiten entfaltet?*

Antwort:

Grundsätzlich kann eine Datenübermittlung im Sinne des Art. 33 Abs. 10 PAG-E nur im örtlichen und sachlichen Zuständigkeitsbereich der bayerischen Polizei erfolgen.

Darüber hinaus kann ich aufgrund des fehlenden datenschutzrechtlichen Bezugs dieser Frage keine Aussage treffen.

Frage:

- c) *Obschon der Gesetzestext in Abs. 10 Satz 4 davon spricht, dass eine flächendeckende Überwachung unzulässig ist, läuft die Norm Ihres Erachtens nicht gerade doch darauf hinaus?*

Antwort:

Art. 33 Abs.10 PAG-E stellt auf Kamerasysteme an oder in den in Art. 13 Abs. 1 Nr. 3 PAG genannten Objekten ab. Beachtet man, dass u.a. auch Verkehrs- und Versorgungsanlagen, öffentliche Verkehrsmittel, Amtsgebäude, Rundfunkanstalten, konsularischen Vertretungen, militärische Einrichtungen und sogar Privatwohnungen gefährdeter Personen (vgl. Schmidbauer/Steiner/Schmidbauer, 6. Aufl. 2023, PAG Art. 13 Rn. 35) zu diesen Objekten gehören, wird deutlich, welches räumliche Ausmaß die geplante Zugriffsmöglichkeit haben kann. Die große Zahl an Möglichkeiten, auf Videoaufzeichnungen zugreifen zu können, halte ich aus datenschutzrechtlicher Sicht für problematisch. In diesem Zusammenhang ist zu beachten, dass bereits im Jahr 2012 allein ÖPNV-Einrichtungen in Bayern mit insgesamt 5.347 Kameras überwacht wurden (siehe LT-Drucksache 16/15571 vom 22. Februar 2013; schriftliche Anfrage der Abgeordneten Christine Kamm vom 24. September 2012). Diese Anzahl hat sich in den letzten Jahren noch deutlich erhöht. Bereits die potentielle Möglichkeit, auf alle diese Videoüberwachungsanlagen präventivpolizeilich zugreifen zu können, schafft insbesondere im urbanen Bereich einen Überwachungsdruck, der aus datenschutzrechtlicher Sicht abzulehnen ist.

Auch der pauschale Hinweis auf die Unzulässigkeit einer flächendeckenden Überwachung in Satz 4 ändert nichts an meiner grundsätzlichen Einschätzung, da die Installation neuer Videoüberwachungsanlagen von öffentlichen und v.a. auch privaten Betreibern materiell nicht in der Hand der bayerischen Polizei liegt. Dementsprechend stellt der Hinweis in seiner jetzigen Formulierung lediglich eine unbeeinflussbare Absichtsbekundung dar und hat letztlich datenschutzrechtlich nur einen begrenzten Mehrwert. Als ausreichende und ausgleichende Begrenzung der zu befürchtenden flächendeckenden und lückenlosen Überwachungssituation kann er jedenfalls nicht

verstanden werden. Die Gefahr einer ausufernden Ausweitung der polizeilichen Zugriffsmöglichkeit auf Daten von Videoüberwachungsmaßnahmen Dritter ließe sich auf normativer Seite wirksam etwa durch einschränkende Regelungen zum Rechtsgüterschutz und eine Erhöhung der Anordnungsvoraussetzungen begegnen.

Frage:

d) *Auch wenn nach der Gesetzesbegründung für die Betreiber datenschutzrechtliche Verpflichtungen zur Kenntlichmachung und Transparenz gelten, wie wird sichergestellt, dass diese auch eingehalten worden sind und welche Konsequenzen bringt es für die Übermittlungspflicht mit sich, wenn diese doch nicht eingehalten wurden?*

Antwort:

Die Videoüberwachung öffentlicher Stellen ist gemäß Art. 24 Abs. 2 BayDSG durch geeignete Maßnahmen erkennbar zu machen und der Verantwortliche ist anzugeben, soweit dieser nicht aus den Umständen hervorgeht. Auch für private Betreiber gelten entsprechende Transparenzpflichten (Art. 5 Abs. 1 Buchst. a, Art. 12 f. DSGVO). Das Transparenzgebot muss für die gesamte Dauer der Videoüberwachung beachtet werden.

Bezüglich der Polizei verweist Art. 33 Abs. 10 Satz 7 PAG-E insoweit auf Art. 33 Abs. 6 PAG, wonach die Polizei in geeigneter Weise auf die Aufnahmen und Aufzeichnungen hinzuweisen hat, soweit diese nicht offenkundig sind oder Gefahr im Verzug besteht. Ergänzend verpflichtet Art. 33 Abs. 10 Satz 6 PAG-E die Polizei u.a. dazu, im Regelfall die Betreiber über deren Pflichten nach dem BayDSG zu unterrichten („Die Betreiber sollen ... informiert werden“). Dies müsste eine regelmäßige Unterrichtung über die Transparenzpflichten des Betreibers nach Art. 24 Abs. 2 BayDSG beinhalten.

Wie bereits angedeutet, ist der Entwurf insoweit defizitär, als nichtöffentliche Betreiber typischerweise keinen Pflichten nach dem BayDSG unterliegen.

Solange gesetzlich nicht klargestellt ist, dass die Polizei nur auf von Dritten rechtmäßig erhobenes Videomaterial zugreifen darf, besteht im Übrigen die Gefahr, dass Verstöße des Betreibers gegen die ihm obliegenden Transparenzvorschriften keine Auswirkungen auf die Übermittlungspflicht nach Art. 33 Abs. 10 PAG-E haben.

Frage:

- e) *Wie beurteilen Sie vor dem Hintergrund der Änderung des Art. 33 die Angemessenheit der Fristen nach Art. 33 Abs. 8 zur Löschung der erhobenen Daten*

Antwort:

Im Rahmen der Neuordnung des bayerischen Polizeirechts im Jahr 2018 wurde die Höchstspeicherfrist polizeilicher Videoüberwachungen von damals drei Wochen auf maximal zwei Monate erhöht. Schon damals habe ich diese Verlängerung des Speicherzeitraums bedauert, da sich für mich die Erforderlichkeit insbesondere im Bereich der Gefahrenabwehr nicht erschloss (siehe auch 28. TB, Nr. 4.3; abrufbar unter <https://www.datenschutz-bayern.de/tbs/tb28/k4.html#4.3>). In der Folge konnte ich in der polizeipraktischen Umsetzung der Befugnis jedoch erreichen, dass bei polizeilichen Videoüberwachungsmaßnahmen die zulässige Höchstspeicherdauer von zwei Monaten im Grundsatz auf maximal 21 Tage begrenzt wurde (siehe auch 30. TB, Nr. 5.2, abrufbar unter <https://www.datenschutz-bayern.de/tbs/tb30/k5.html#5.2>). Aus den Erfahrungen meiner Prüftätigkeit kann ich auch aktuell bestätigen, dass sich diese zeitliche Einhegung als zweckorientiert und verhältnismäßig erwiesen hat und auch von polizeipraktischer Seite als ausreichend bewertet wird. Zudem lässt sich konstatieren, dass sich erfahrungsgemäß der Datenverarbeitungszweck durch längere Speicherzeiträume insgesamt schwerpunktmäßig von der Gefahrenabwehr hin zur Straf- und Ordnungswidrigkeitenverfolgung verschiebt. Um den Gleichklang mit bestehenden Rechtsvorschriften (wie Art. 24 BayDSG) zu wahren und eine in der Gesamtschau verlängerte Speichermöglichkeit durch die Polizei zu unterbinden, konnte ich insofern die nun vorliegende Klarstellung in Art. 33 Abs. 10 Satz 7 PAG-E erreichen, wonach sich die Speicherungsfrist des Art. 33 Abs. 8 PAG nach dem Zeitpunkt der ursprünglichen Datenerhebung durch den Betreiber richtet und nicht danach, wann die Polizei die Daten erhalten hat.

Unabhängig davon würde ich natürlich auch weiterhin aus den oben genannten Gründen eine gesetzliche Herabsetzung der Höchstspeicherfrist polizeilicher Videoüberwachungen ausdrücklich begrüßen.

3. Art. 41, 44, 45 PAG-E

Fragen:

- a) *Wie beurteilen Sie die Änderungen im PAG?*
- b) *Sind die Maßgaben des Bundesverfassungsgerichts ausreichend umgesetzt?*

Antwort:

Die geplanten Neuregelungen in Art. 41 Abs. 4 Satz 2, Art. 44 Abs. 1 Satz 5 und Art. 45 Abs. 3 Satz 4 PAG-E setzen die Vorgaben des Beschlusses des Bundesverfassungsgerichts unter Rn. 131 ff. um. Die dortigen Ausführungen messen das vorbereitende Betreten der Wohnung an den verfassungsrechtlichen Vorgaben des Art. 13 Abs. 7 GG, da die Vorschriften des Art. 13 Abs. 2, 3 und 4 GG jeweils keine tauglichen verfassungsrechtlichen Grundlagen für derartige Maßnahmen bilden. Demnach muss eine konkretisierte Gefahr für ein Rechtsgut von besonderem Gewicht vorliegen. Mit der angepassten Formulierung wird klargestellt, dass die vorbereitende Wohnungsbetretung den gleichen Voraussetzungen unterliegt wie die jeweilige Maßnahme selbst. Diese Voraussetzungen genügen dem verfassungsrechtlichen Anspruch.

4. Art. 49 PAG-E

Fragen:

- a) *Sind die Sicherungsmaßnahmen zum Schutz des Kernbereichs ausreichend umgesetzt, um ein Eindringen in den Kernbereich zu verhindern und eine Weiterverarbeitung von Kernbereichsdaten zu unterbinden?*
- b) *Wie beurteilen Sie insgesamt die Umsetzung der Maßgaben des BVerfG und für den Fall, dass Sie die Umsetzung als unzureichend erachten sollten, wie was wären Ihres Erachtens verfassungskonforme Alternativen?*

Antwort:

Auch die geplante Neuregelung zum Kernbereichsschutz in Art. 49 PAG-E setzt die Vorgaben des Beschlusses um. Das Bundesverfassungsgericht statuiert, dass der

Gesetzgeber Maßnahmen zum Kernbereichsschutz auf Erhebungs- und auf Auswertebene vorsehen muss (Rn. 109 und 117).

Auf Erhebungsebene muss zunächst von Gesetzes wegen ausgeschlossen sein, dass der Kernbereich Ziel staatlicher Ermittlungen ist. Weiter ist bei verletzungsgeneigten Maßnahmen durch eine vorgelagerte Prüfung sicherzustellen, dass die Erfassung von kernbereichsrelevanten Situationen oder Gesprächen jedenfalls insoweit ausgeschlossen ist, als sich diese mit praktisch zu bewältigendem Aufwand im Vorfeld vermeiden lässt. Außerdem ist grundsätzlich der Abbruch der Maßnahme vorzusehen, wenn erkennbar wird, dass eine Überwachung in den Kernbereich privater Lebensgestaltung eindringt.

Die geplante Neuregelung setzt nunmehr die verfassungsrechtlichen Vorgaben zur Ausnahme vom Abbruchgebot (Rn. 115) um, insbesondere genügt nur eine Gefahr für Leib oder Leben der V-Person oder des verdeckten Ermittlers als Rechtfertigung für den unterbliebenen oder verzögerten Abbruch. Auch die vom BVerfG aufgeführten Dokumentationspflichten (Rn. 119 ff.) werden umgesetzt.

5. Art. 61a PAG-E

Fragen:

- a) *Sehen Sie die Entscheidung des BVerfG vom 16.02.2023 (Az. 1 BvR 1547/19, 1 BvR 2634/20) mit der vorgelegten Norm ausreichend umgesetzt? Falls nicht, was sind Ihre Kritikpunkte an der geplanten gesetzlichen Umsetzung?*
- b) *Sind insbesondere die Einschränkungen hinsichtlich der zu schützenden Rechtsgüter und der zugelassenen Methoden der Datenverarbeitung ausreichend, um das Eingriffsgewicht der Maßnahme auf ein verfassungsrechtlich vertretbares Niveau zu senken?*
- c) *Wie beurteilen Sie die Aufnahme des Rechtsguts der „Eigentums- oder Vermögenswerte, wenn tatsächliche Anhaltspunkte für eine drohende gewerbsmäßige oder bandenmäßige Schädigung dieser Rechtsgüter vorliegen, die geeignet ist,*

den Rechtsfrieden in erheblicher Weise zu stören“, insbesondere hinsichtlich des Ziels der Gefahrenabwehr bezüglich organisierter bzw. bandenmäßiger Schädigung von Rechtsgütern.

- e) *Welche Risiken sehen Sie beim geplanten Einsatz von VeRA für die Bürgerinnen und Bürger, insbesondere im Hinblick auf etwaige Grundrechtsverletzungen?*

Antwort:

Ich erlaube mir, die Art. 61a PAG-E betreffenden Fragen a), b), c) sowie e) aufgrund deren inneren Zusammenhangs einheitlich zu beantworten:

- (1) Ich hatte in der Vergangenheit wiederholt Gelegenheit, zur geplanten Einführung der verfahrensübergreifenden Recherche- und Analyseplattform („VeRA“) Stellung zu nehmen. Dabei hatte ich stets darauf hingewiesen, dass eine automatisierte Datenverarbeitung – wie sie mit VeRA beabsichtigt ist – im Vergleich zu einer händischen Auswertung vorhandener Daten ein enormes Eingriffsgewicht mit immenser Streubreite aufweist und auch im Rahmen der Überwachungsgesamtrechnung Bedeutung erlangen kann. Dementsprechend habe ich meine datenschutzrechtlichen Vorbehalte stets klar geäußert.

Das Bundesverfassungsgericht hat nunmehr in seiner Entscheidung vom 16. Februar 2023 ausdrücklich bestätigt, dass mit einer automatisierten Anwendung zur Datenanalyse oder -auswertung in die informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 Grundgesetz – GG) aller eingegriffen wird, deren Daten bei diesem Vorgang personenbezogen Verwendung finden, da mit der automatisierten Auswertung gespeicherter Daten der Gesetzgeber eine weitere Nutzung früher erhobener Daten über den ursprünglichen Anlass hinaus erlaubt. Vor allem aber stellt das Bundesverfassungsgericht deutlich heraus, dass ein Grundrechtseingriff nicht nur in der weiteren, zusammenführenden Verwendung vormals getrennter Daten liegt. Vielmehr ergibt sich ein weiterer Grundrechtseingriff gerade in der Erlangung besonders grundrechtsrelevanten neuen Wissens, das durch die automatisierte Datenanalyse oder Datenauswertung geschaffen werden kann (BVerfG, a.a.O., Rn. 50). Die automati-

sierte Anwendung könne die Arbeitsweise und Erkenntnismöglichkeiten der Polizei somit entscheidend verändern und so auch das Gewicht der individuellen Beeinträchtigung bedeutend erhöhen. Der verfassungsrechtliche Grundsatz der Zweckbindung genüge dem Eingriffsgewicht dann für sich genommen nicht mehr (BVerfG, a.a.O., Rn. 70). Die Rechtfertigung eines solchen gesonderten Grundrechtseingriffs setzt vielmehr eine gesetzliche Ermächtigung voraus, die einen legitimen Zweck verfolgt und auch im Übrigen dem Grundsatz der Verhältnismäßigkeit genügen muss. Im Zusammenhang mit einer automatisierten Datenanalyse oder -auswertung hat das Bundesverfassungsgericht aber nunmehr auch klargestellt, dass die verfassungsrechtlichen Anforderungen an die Rechtfertigung variieren. Es ergeben sich spezielle Anforderungen aus dem Gebot der Verhältnismäßigkeit im engeren Sinne. Wie streng diese Anforderungen im Einzelnen sind, bestimmt sich nach dem Eingriffsgewicht der Maßnahme (BVerfG, a.a.O., Rn. 54). Das Eingriffsgewicht einer automatisierten Datenanalyse und -auswertung ergibt sich zum einen aus dem Gewicht der vorausgegangenen Datenerhebungseingriffe. Zum anderen habe die automatisierte Datenanalyse oder -auswertung potenziell ein Eigengewicht, so dass weitergehende Rechtfertigungsanforderungen gelten. Entsprechend variabel sind die Anforderungen an die Eingriffsvoraussetzungen, also insbesondere an die Eingriffsschwelle, das zu schützende Rechtsgut und die Sicherung von Transparenz, Rechtsschutz und aufsichtlicher Kontrolle, deren Regelung dem Grundsatz des Gesetzesvorbehalts, dem Gebot der Normenklarheit und dem Bestimmtheitsgebot genügen muss (BVerfG, a.a.O., Rn. 71).

- (2) Nach den vom Bundesverfassungsgericht dargelegten generellen Maßstäben erachte ich das spezifische Eingriffsgewicht der nach **Art. 61a Abs. 1 PAG-E** formulierten Befugnis zur Datenanalyse oder -auswertung durch VeRA als **sehr hoch**, so dass diese Regelungen von Verfassungs wegen strengen Eingriffsvoraussetzungen genügen müssen.
- (a) Aus meiner Sicht knüpft der Entwurf der Rechtsprechung des Bundesverfassungsgerichts entsprechend zutreffend den Einsatz von VeRA in Art. 61a Abs. 1 PAG-E an den Schutz besonders gewichtiger Rechtsgüter und erfordert das Vorliegen einer konkreten oder drohenden Gefahr, mithin, in der Diktion

des Bundesverfassungsgerichts, mindestens einer hinreichend konkretisierten Gefahr.

- (b) Gleichwohl halte ich die mögliche Einbeziehung aller bei der Polizei automatisiert verarbeiteten Daten unter datenschutzrechtlichen Aspekten für bedenklich. So wird der Umfang der potenziell in die Datenanalyse oder Datenauswertung einbezogenen Daten nicht maßgeblich durch Art. 61a PAG-E begrenzt. Vielmehr sollen alle automatisierten Verfahren im Sinn des Art. 64 Abs. 1 Satz 1 PAG potenziell einbezogen werden können. Aus der Gesetzesbegründung (S.27) ergibt sich, dass „alle gem. Art. 54 Abs. 1 gespeicherten Daten, mithin solche zur polizeilichen Aufgabenerfüllung, zur zeitlich befristeten Dokumentation oder sonstigen Vorgangsverwaltung erfasst“ sind. Es soll also der volle Datenbestand der Polizei umfasst werden. Aus datenschutzrechtlicher Sicht halte ich jedoch eine möglichst konkrete Begrenzung für vorzugswürdig. Insbesondere stehe ich nach wie vor einer Einbeziehung von Daten aus dem „Integrationsverfahren Polizei“ (IGVP), in welchem aktuell Daten nach Art. 54 Abs. 1 PAG gespeichert werden, kritisch gegenüber (vgl. hierzu unten Nummer 5 (3)(b)).

Nachdem zunächst unklar war, ob nicht sogar Daten aus dem Personal- und Stellenverwaltungssystem (VIVA) als Quelldatei für Datenverarbeitungen nach Art. 61a Abs. 1 Satz 1 PAG-E einbezogen werden sollten, hatte ich darauf hingewiesen, dass Personalaktendaten gemäß § 50 Satz 3 Beamtenstatusgesetz, Art. 103 Satz 1 Bayerisches Beamtengesetz (BayBG) nur streng zweckgebunden, insbesondere zu Zwecken der Personalverwaltung und Personalwirtschaft, verarbeitet werden dürfen. In personeller Hinsicht beschränkt Art. 103 Satz 2 BayBG die Verarbeitungsbefugnis auf Beschäftigte, die mit Personalangelegenheiten betraut worden sind. Art. 108 BayBG lässt Auskünfte aus der Personalakte ohne Einwilligung der betroffenen Beschäftigten nur in eng begrenzten Ausnahmen zu. Diese Vorschriften gelten für tarifvertraglich Beschäftigte grundsätzlich entsprechend (Art. 145 Abs. 2 BayBG) und finden insbesondere auch Anwendung, wenn Personalaktendaten mittels automatisierter Verfahren verarbeitet werden, Art. 111 Abs. 1 Satz 1 BayBG. Erfreulicherweise wurde zwischenzeitlich in der Gesetzesbegründung klargestellt, dass ein Abgleich interner Personaldatenbanken aus dem Anwendungsbereich der Norm ausschei-

det (Gesetzesbegründung, S. 24). Auch Kommunikation, welche nicht dem Zweck der polizeilichen Aufgabenerfüllung dient (z.B. jene der Personalräte), scheidet aus (Gesetzesbegründung, S. 28). Dementsprechend ist aber auch tatsächlich zu gewährleisten, dass dienstlicher E-Mail-Verkehr der Personalstellen sowie der zur Verschwiegenheit verpflichteten internen „Geheimnisträger“ (insbesondere Personalräte, Schwerbehindertenvertretungen und Gleichstellungsbeauftragte) entsprechend den Ausführungen in der Gesetzesbegründung **normenklar** von einem Abgleich ausgenommen wird.

- (c) Art. 61a Abs. 3 Nr. 4 PAG-E sieht auch eine Einbeziehung der Einsatzdokumentationssysteme vor. Aus der Gesetzesbegründung (S. 28) ergibt sich, dass es hierbei um Systeme geht, die den Einsatzleitstellen und Führungsstäben zur Verfügung stehen. Da nach meiner Kenntnis in derartigen Dateien auch viele Personen gespeichert werden, die weder einer Straftat oder Ordnungswidrigkeit verdächtig oder von polizeilichen Eingriffsmaßnahmen betroffen, sondern Zeugen, Geschädigte, Auskunftspersonen etc. sind, habe ich bzgl. der Einbeziehung dieser Daten ähnliche Bedenken, wie ich sie bezogen auf IGVP äußere (vgl. hierzu unten Nummer 5 (3)(b)). Hinzukommt, dass nach meiner Erfahrung derartige Dateien oftmals auch im Zusammenhang mit Versammlungsgeschehen verwendet werden. Dies bedeutet, dass sich auch die Frage stellt, ob und inwieweit eine Verwendung von Daten von Versammlungsanmeldern und Versammlungsleitern den Schutzbereich des Art. 8 Grundgesetz (GG) berührt.
- (3) Im Unterschied zum Referentenentwurf schätze ich vor allem aber das **Eingriffsgewicht von Maßnahmen nach Art. 61a Abs. 2 PAG-E als sehr hoch ein:**
- (a) Dabei erkenne ich die grundsätzlichen Bestrebungen des Entwurfs durchaus an, das Eingriffsgewicht durch die Beschränkung der Quellsysteme nach Art. 61a Abs. 3 PAG-E für Maßnahmen nach Art. 61a Abs. 2 PAG-E zu senken. Entsprechendes gilt für die Beschränkung der zugelassenen Datenarten (Art. 61a Abs. 2 Sätze 3 und 4 PAG-E), den Verzicht auf die Verwendung selbstlernender Systeme, die Beschränkung der Ergebnisanzeige (Art. 61a Abs. 3 Satz 2 PAG-E) sowie die beabsichtigte Schulung des eingesetzten Per-

sonals (Art. 61a Abs. 4 PAG-E).

- (b) Gleichwohl genügen diese Ansätze aus meiner Sicht nicht, um das Eingriffsgewicht der mit VeRA verbundenen Befugnis zur Datenanalyse oder -auswertung nach Art. 61a Abs. 2 PAG-E als nicht sehr hoch oder gar gering einzuordnen:

Hier ist nämlich besonders zu sehen, dass die auch nach Art. 61a Abs. 3 Satz 1 PAG-E aufgezählten automatisierten Verfahren, die mittels VeRA nach Art. 61a Abs. 2 PAG-E automatisiert analysiert oder ausgewertet werden können, schon für sich genommen von solcher Tragweite und solchem Umfang sind, dass ein entsprechend hohes Eingriffsgewicht mit ihrer Einbeziehung verbunden ist. Eine „deutliche Einschränkung der Arten und des Umfangs“ (Gesetzesbegründung, S. 26) kann ich aufgrund der Mächtigkeit der einbezogenen Datenquellen kaum erkennen. Die Einbeziehung von IGVP als Quelldatei habe ich in der Vergangenheit stets abgelehnt. Auch vor dem Hintergrund des Urteils des Bundesverfassungsgerichts vom 16. Februar 2023 sehe ich mich nicht veranlasst, von dieser Forderung abzuweichen, sondern eher noch bestärkt. Das Gericht hatte in seiner Entscheidung nämlich betont, dass durch die Einbeziehung der Daten aus der Vorgangsbearbeitung gerade sehr viele Daten von Betroffenen einbezogen werden könnten, die keinen Anlass für Maßnahmen einer vorbeugenden Bekämpfung schwerer Straftaten geben.

Allein für IGVP wurde mir auf eine Anfrage hin vom Bayerischen Staatsministerium des Innern, für Sport und Integration berichtet, dass zum damaligen Auswertzeitpunkt (30. August 2022) **38.659.637 „Vorgangspersonen“** in **21.849.507 Vorgängen** erfasst waren. Allein für das Jahr 2021 wurden insgesamt 5.471.643 „Vorgangspersonen“ in 2.470.342 Vorgängen erfasst. **Die Mehrzahl der gespeicherten Personen war weder einer Straftat oder Ordnungswidrigkeit verdächtig oder von polizeilichen Eingriffsmaßnahmen betroffen** (sog. „B-Personen“), sondern Zeugen, Geschädigte, Auskunftspersonen etc. (sog. „Z-Personen“). **Das Verhältnis zwischen B-Personen und Z-Personen lag im Jahr 2021 bei ca. 1:2, bezogen auf den IGVP Gesamtbestand bei 2:3.** Auch wenn davon auszugehen ist, dass Daten einer größeren Anzahl an Personen in mehreren Vorgängen erfasst sind und die tatsächliche

Anzahl der erfassten Personen deutlich kleiner ist als die Anzahl der „Vorgangspersonen“, ist immer noch von äußerst vielen Betroffenen auszugehen. Diese Entwicklung dürfte sich in den vergangenen Jahren noch weiter fortgesetzt haben.

Erschwerend kommt hierbei hinzu, dass die Polizei nach Art. 54 Abs. 1 PAG personenbezogene Daten unter sehr niedrigen Voraussetzungen zum Zwecke der Aufgabenerfüllung, der Dokumentation oder der Vorgangsverwaltung speichern oder anderweitig verarbeiten kann. Damit hat die Polizei theoretisch ohne Weiteres die Möglichkeit, etwa durch eine extensivere Dokumentation ihres Handelns das Volumen der in IGVP gespeicherten Daten eigenständig und nur wenig normativ begrenzt zu erhöhen. Im Kontext einer automatisierten Datenanalyse oder -auswertung erhöht sich das damit verbundene Eingriffsgewicht nochmals enorm.

- (c) Bei einer gesetzlich zugelassenen Methode einer Auswertung großer Datenmengen insbesondere auch auf statistische Zusammenhänge hin, ist außerdem eine **ausreichende Datenqualität sicherzustellen** (BVerfG, a.a.O., Rn. 91 ff.).

Aufgrund meiner Prüfungserfahrungen der letzten Jahre möchte ich darauf hinweisen, dass die Qualität der in polizeilichen Dateien enthaltenen Daten nach meiner Einschätzung durchaus verbesserungswürdig ist. Regelmäßig veranlassen mich Bürgereingaben oder anlasslose Prüfungen dazu, bei der Polizei Änderungen von Speicherungen zu erbitten, etwa wegen der falschen Zuordnung von Personenkategorien bei eingestellten Strafverfahren ohne polizeilichen Restverdacht oder einer zu langen Speicherdauer zu Dokumentationszwecken. Ich darf allein betreffend IGVP beispielsweise auf meine Tätigkeitsberichte der letzten zehn Jahre, insbesondere 31. TB 2021 Nr. 3.5, 30. TB 2020 Nr. 5.4, 29. TB 2019 Nr. 3.2, 28. TB 2017/2018 Nr. 4.4.1, 27. TB 2015/2016 Nr. 3.6.4 und 27. TB 2013/2014 Nr. 3.5.1, 3.5.2, 3.5.3) hinweisen (abrufbar unter https://www.datenschutz-bayern.de/inhalte/taetig_t.htm).

Aus diesem Grund habe ich die Sorge, dass die verfassungsrechtliche Anforderung nach einer ausreichenden Datenqualität in der Praxis nur schwer erfüllt

werden wird. Den mir gegenüber im Verlauf des Verfahrens geäußerten Hinweis, die Datenqualität der angebundenen Verfahren habe keine Bedeutung für das Eingriffsgewicht der mit VeRA verbundenen Datenverarbeitungen, da es sich allenfalls um ein Vollzugsproblem handele, halte ich nicht für tragfähig. Wie schwer Eingriffe durch automatisierte Datenanalyse oder Datenauswertung wiegen, hängt insgesamt auch davon ab, wie fehleranfällig die eingesetzte Datenauswertungstechnologie ist und ob gegebenenfalls Vorkehrungen zur Entdeckung und Korrektur von Fehlern getroffen sind. Das betrifft freilich nicht nur die unmittelbaren Daten(weiter)verarbeitungen, sondern auch die Qualität der Ausgangsdaten.

- (d) Ursprünglich war unklar, ob die Beschränkung des Art. 61a Abs. 3 Satz 1 PAG-E auch die Auswertungsmöglichkeit für betreffende Dateisysteme erlaubt, die außerhalb des Landesbestandes der bayerischen Polizei liegen. Diese Unklarheit wurde zwischenzeitlich durch eine Klarstellung in Art. 61a Abs. 1 PAG-E behoben. Danach muss es sich um „eigene“ automatisierte Verfahren der bayerischen Polizei handeln. Dies betrifft allerdings nur die automatisierte Anbindung. Der Abruf und der spätere **manuelle Import landesfremder Daten** soll auch weiterhin über die einschlägigen Normen des PAG **möglich sein**. In den Bereich der Recherche und Analyse durch VeRA können daher 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.

Im Ergebnis kann damit nicht ausreichend eingegrenzt werden, welche Datenquellen für elaborierte Datenweiterverarbeitungen durch VeRA letztendlich zur Verfügung stehen werden.

- (e) Art. 61a Abs. 5 Nrn. 1 und 2 PAG-E schließen zwar erfreulicherweise eine automatisierte Entscheidungsfindung und die Verwendung selbstlernender Systeme aus. Gleichwohl schließt dies nicht automatisch auch komplexere Formen des Datenabgleichs aus. Ich gehe davon aus, dass insbesondere auch offene

Suchvorgänge zulässig sein sollen. Die Datenanalyse oder -auswertung kann auch darauf zielen, allein statistische Auffälligkeiten in den Datenmengen zu entdecken, aus denen dann, möglicherweise weitere Schlüsse gezogen werden. Auch wenn die Gesetzesbegründung darauf hinweist, dass die neuen Erkenntnisse – wie bisher auch – anschließend durch Polizeibeamte bewertet werden, vermag dies aus den vorstehenden Gründen keine erhebliche Reduktion des Eingriffsgewichts zu vermitteln. Für das Eingriffsgewicht einer Norm sind auch nicht die bloße Vorstellung des Gesetzgebers von der begrenzten Reichweite einer Befugnis oder der Wille der Verwaltung, von den rechtlichen Möglichkeiten einer Befugnis nicht umfassend Gebrauch zu machen, maßgeblich. Das Gewicht ist vielmehr nach den rechtlich geschaffenen Eingriffsmöglichkeiten zu beurteilen (BVerfG, a.a.O., Rn. 149).

- (f) Auch soweit die Gesetzesbegründung eine hinreichende externe datenschutzrechtliche Kontrolle durch die Vorlage der zugehörigen Errichtungsanordnung mit Datenschutzfolgenabschätzung nach Art. 64 PAG gewährleistet sieht, vermag ich hierin keine relevante Reduktion des Eingriffsgewichts zu erkennen.

Denn Art. 64 Abs. 1 Satz 2 PAG wie auch Art. 64 Abs. 2 Satz 6 PAG sehen lediglich eine Informationspflicht vor. Ein Veto-Recht oder andere effektive Kontroll- und insbesondere Abhilfebefugnisse sind auch vor dem Hintergrund von Art. 34 Abs. 1 Satz 1 Bayerisches Datenschutzgesetz (BayDSG) für den Bayerischen Landesbeauftragten für den Datenschutz nicht vorhanden.

- (4) All dies lässt mich zu dem Ergebnis gelangen, **dass das Eingriffsgewicht auch von Maßnahmen nach Art. 61a Abs. 2 PAG-E als schwer einzustufen ist.**

Ermöglicht die automatisierte Anwendung einen eigenständig schweren Eingriff in die informationelle Selbstbestimmung der Betroffenen, ist dies nur unter engen Voraussetzungen zu rechtfertigen, wie sie allgemein für eingriffsintensive heimliche Überwachungsmaßnahmen gelten. Heimliche Überwachungsmaßnahmen, die tief in das Privatleben hineinreichen, sehen Benachrichtigungspflichten vor und sind **nur zum Schutz besonders gewichtiger Rechtsgüter**

zulässig (Leib, Leben und Freiheit der Person, Bestand oder Sicherheit des Bundes oder eines Landes, u.U. der Schutz von Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist). **Auch der Eingriffsanlass** muss dann 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**.

- (a) Demgemäß scheiden Maßnahmen nach **Art. 61a Abs. 2 Satz 1 Nr. 1 i.V.m. Abs. 1 Satz 1 PAG-E von vornherein aus**, da sich diese der Verhütung und Unterbindung von Straftaten dienenden Maßnahmen **noch im Vorfeld einer konkretisierten bzw. drohenden Gefahr** bewegen und damit die vom Bundesverfassungsgericht gestellten Anforderungen nicht erfüllen.

Auch die in Art. 61a Abs. 2 Satz 1 Nr. 1 PAG-E vorgesehene Beschränkung auf besonders schwere Straftaten nach § 100b StPO genügt den verfassungsrechtlichen Anforderungen an die Eingriffsschwelle besonders gewichtiger Rechtsgüter nicht. Zwar umfassen die in § 100b StPO genannten Tatbestände durchaus auch den Schutz besonders gewichtiger Rechtsgüter. Jedoch gilt das gerade nicht für alle der dort genannten Straftatbestände, so dass die verfassungsrechtlichen Anforderungen nicht in jedem Fall gewahrt sein müssen.

- (b) Dieser Befund gilt im **Ergebnis auch für Maßnahmen nach Art. 61a Abs. 2 Satz 1 Nr. 2 PAG-E**. Zwar wird die Eingriffsschwelle hier an das Vorliegen einer konkreten oder einer drohenden Gefahr geknüpft.

Aber auch hier genügen die in Art. 61a Abs. 2 Satz 1 Buchst. a) bis c) PAG-E genannten Rechtsgüter nicht in allen Fällen den verfassungsrechtlichen Anforderungen an den Schutz besonders gewichtiger Rechtsgüter. Zwar mag man Buchst. d) noch unter den Schutz von Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, subsumieren. Aber schon Art. 61a Abs. 2 Satz 1 Nr. 1 a) PAG-E stellt ausdrücklich auf den Schutz der Gesundheit einer Person in solchen Fällen ab, die nicht durch Art. 61a Abs. 1 Satz 1 Nr. 1 PAG-E umfasst sind.

Zudem können auch nicht alle Fälle der Straftaten gegen die sexuelle Selbstbestimmung zwangsläufig unter den Schutz von Leib, Leben oder Gesundheit gefasst werden.

Dass Eigentums- und Vermögenswerte, auch wenn sie gewerbs- oder bandenmäßig begangen werden, im Regelfall nicht zu den besonders gewichtigen Rechtsgütern zu zählen sind, liegt am deutlichsten auf der Hand.

- (c) Soweit man an der derzeitigen Ausgestaltung von Art. 61a Abs. 2 PAG-E, insbesondere der Anbindung von IGVP, festhalten möchte, genügen die derzeitigen Eingriffsschwellen nicht den verfassungsrechtlichen Schranken.

Aus meiner Sicht ließe sich eine hinreichende Beschränkung des Eingriffsgewichts nur durch den normenklar festgeschriebenen Ausschluss von IGVP sowie zukünftiger Systeme oder Dateien, die auf Art. 54 Abs. 1 PAG beruhen, erreichen.

Frage:

- d) *Wie beurteilen Sie vor dem Hintergrund, dass die Polizeisoftware VeRA des US-Herstellers Palantir bei Experten bekanntlich umstritten ist,*
- *nicht zuletzt Europol den Einsatz von Palantir beendet und*
 - *das Bundesministerium des Innern und für Heimat den Einsatz und die Anwendung der Software von Palantir beim BKA und bei der Bundespolizei gestoppt hat,*
 - *sowie die Innenministerkonferenz mit Beschluss vom Juni 2023 mehrheitlich von der weiteren Projektierung und Umsetzung der Software aus der ursprünglichen Rahmenvereinbarung Abstand genommen hat,*

das Festhalten Bayerns an der Software vor der möglichen Notwendigkeit einer bundeseinheitlichen Kompatibilität, um Ermittlungsergebnisse effizient zu generieren?

Antwort:

Unabhängig davon, dass mir Einzelheiten zu den o.g. Entwicklungen nicht bekannt sind, betrifft die Frage, ob Bayern vor dem Hintergrund der genannten Entwicklungen auf europäischer und Bundesebene an seinem Vorhaben zur Einführung von VeRA festhalten sollte, in erster Linie keine datenschutzrechtliche, sondern vielmehr eine politische Gestaltungsentscheidung. Aus fachlicher Sicht kann ich daher über meine vorgenannten Ausführungen keine weitere Einschätzung dazu abgeben.

Frage:

- e) *Welche Risiken sehen Sie beim geplanten Einsatz von VeRA für die Bürgerinnen und Bürger, insbesondere im Hinblick auf etwaige Grundrechtsverletzungen?*

Antwort:

Siehe Antwort oben zu Frage a).

Frage:

- f) *Wie sehen Sie den Einsatz der Software des US-Herstellers vor dem Hintergrund einer „digitalen Souveränität“ Deutschlands und Europas in sicherheitsrelevanten Bereichen?*

Antwort:

Aus datenschutzrechtlicher Sicht spielt der Hersteller der zu verwendenden Software zunächst keine unmittelbare Rolle. Die Geltung rechtlicher Rahmenbedingungen, insbesondere der technisch-organisatorischen Anforderungen, ist bei jeglicher Software zu beachten.

6. Abschließende Einschätzung

Meine wesentlichen Anmerkungen zu dem vorliegenden Gesetzentwurf habe ich oben ausführlich dargelegt. Abschließend möchte ich noch Folgendes anmerken:

In den letzten Jahren wurden die polizeilichen Befugnisse konsequent erweitert und auch in diesem Entwurf sind neue Befugnisse enthalten, die, wie vor allem Art. 33 Abs. 10 PAG-E, erwarten lassen, dass der Polizei noch mehr Datenmaterial zur Verfügung steht als bisher. Hinzukommt, dass aufgrund der fortschreitenden Digitalisierung Bürgerinnen und Bürger immer mehr Daten über sich produzieren, auf die die Polizei im Rahmen ihrer Aufgabenerfüllung ggf. zugreifen kann. Durch die geplante Einführung einer datenbank- und formatübergreifenden Recherche innerhalb der polizeiinternen Datenbestände zur Unterstützung der Analyse und Auswertung erhalten derartige Daten einen anderen „Wert“ und das Eingriffsgewicht der bloßen Speicherung erhöht sich.

Vor diesem Hintergrund ist eine isolierte Einführung von VeRA ohne gleichzeitige Anpassung der polizeilichen Datenverarbeitungsregelungen in Art. 54 PAG aus Sicht des Datenschutzes grundsätzlich problematisch.

Ich empfehle daher, die Gelegenheit zu nutzen, die Mitziehklausel (Art. 54 Abs. 2 Satz 3 PAG) ersatzlos zu streichen und Art. 54 Abs. 2 PAG, wie auf Bundesebene, um eine zu dokumentierende Negativprognose zu ergänzen. Auch ist es meines Erachtens angezeigt in Art. 54 Abs. 1 PAG eine Regelhöchstspeicherungsfrist von zwei Jahren sowie die Verpflichtung den Zweck der Speicherung (Aufgabenerfüllung, Vorgangsverwaltung oder Dokumentation) eindeutig und verbindlich festzuhalten, aufzunehmen.

Durch derartige gesetzgeberische Maßnahmen könnte, wenn VeRA eingeführt wird, der vom Bundesverfassungsgericht ins Spiel gebrachten Überwachungsgesamtrechnung aber auch allgemeinen Verhältnismäßigkeitserwägungen etwas Rechnung getragen werden.

Mit freundlichen Grüßen

gez.
Prof. Dr. Thomas Petri
Landesbeauftragter für den Datenschutz