



Thüringer Landesbeauftragter für den Datenschutz und
die Informationsfreiheit (TLfDI), PF 900455, 99107 Erfurt

ggf. Alt-Az:

(bisheriges Aktenzeichen)

Thüringer Landtag
Ausschuss für Inneres, Kommunales und Lan-
desentwicklung
Jürgen-Fuchs-Straße 1

99096 Erfurt

Az: 1100-R1-1082/431-1-11074/2026

Ihre Nachricht vom :
Ihr Zeichen : Drs. 8/2478-II
Bearbeiter/in : Frau Springer
Telefon : +49 (361) 57-3112912
Erfurt, den : 2. Juni 2026

vorab per E-Mail:
poststelle@thueringer-landtag.de

THÜR. LANDTAG POST
02.06.2026 13:14
1702312026

Thüringer
Landtag
VORLAGE
8/1763

zu Drs. 8/2478

Zweites Gesetz zur Änderung des Polizeiaufgabengesetzes (Drs. 8/2478)

**-hier: Bitte des Ausschusses für Inneres, Kommunales und Landesentwick-
lung um Äußerung gemäß § 112 Abs. 4 der Geschäftsordnung des Thüringer
Landtags**

Sehr geehrter Herr Vorsitzender,
sehr geehrter Herr Dr. Hyckel,

der Thüringer Landesbeauftragte für den Datenschutz und die Informationsfreiheit
(TLfDI) dankt für die Übersendung des Entwurfes des Zweiten Gesetzes zur Ände-
rung des Polizeiaufgabengesetzes (nachfolgend PAG-E) und für die Gelegenheit
zur Stellungnahme gemäß § 112 Abs. 4 der Geschäftsordnung des Thüringer
Landtags.

Der TLfDI möchte aus datenschutzrechtlicher Sicht die nachfolgenden Anmerkun-
gen machen:

Postanschrift: Postfach 900455 Dienstgebäude: Häßlerstraße 8
99107 Erfurt 99096 Erfurt

Telefon: 0361 57-3112900
E-Mail*: poststelle@datenschutz.thueringen.de
Internet: www.tlfdi.de

Umsatzsteuer-Identifikationsnummer: DE338711747

*Die genannte E-Mail-Adresse dient nur für den Empfang einfacher Mitteilungen ohne Signatur/ Verschlüsselung und für mit PGP verschlüsselte Mitteilungen.

I. Vorbemerkung

Polizeiliche Maßnahmen können mit tiefen Eingriffen in die Grundrechte von betroffenen Personen einhergehen. Aus diesem Grund ist das Vorliegen von klaren, bestimmten und verhältnismäßigen gesetzlichen Ermächtigungen im Polizeiaufgabengesetz Thüringen essenziell. Gerade in diesem Bereich ist der Thüringer Gesetzgeber gefordert, diesen hohen Anforderungen zu entsprechen. Die neu geschaffenen Normen müssen einen legitimen Zweck aufweisen und geeignet, erforderlich und angemessen sein. Das Bundesverfassungsgericht hebt in ständiger Rechtsprechung (siehe z.B. BVerfG, Urteil vom 11. März 2008 – 1 BvR 2074/05 –, BVerfGE 120, 378-433, Rn. 168, juris; BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, BVerfGE 141, 220-378 (LT 1-3), Rn. 105ff.; BVerfG, Urteil vom 01. Oktober 2024 - 1 BvR 1160/19 – Rn. 90ff, juris;) die Normenklarheit und Bestimmtheit von Eingriffsbefugnissen nebst der Verhältnismäßigkeit von Eingriffsschwelle und Eingriffsgewicht hervor, deren Umsetzung auch für das vorliegende Gesetz gilt.

Der TLfDI rät davon ab, etwaige Eingriffsschwellen bei polizeilichen Maßnahmen herabzusetzen.

Der Gefahrenbegriff spielt im Thüringer Polizeiaufgabengesetz eine zentrale Rolle. Aus der Sicht des TLfDI sollten deshalb die einschlägigen Definitionen der dem Gesetz zugrundeliegenden Gefahrenbegriffe in den Gesetzestext aufgenommen werden (siehe dazu z.B. § 4 Sächsisches Polizeivollzugsdienstgesetz, Art. 11 Gesetz über die Aufgaben und Befugnisse der Bayerischen Polizei). Zwar werden in der vorliegenden Gesetzesbegründung Ausführungen zu einzelnen Gefahrbegriffen gemacht; diese liegen dem Rechtsanwender in der Praxis aber nicht vor.

An vielen Stellen im Gesetzentwurf wurde zudem der Zusatz „zur Abwehr einer Gefahr für Anlagen der kritischen Infrastruktur oder sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen“ aufgenommen. Insbesondere die Nennung der „sonstigen Anlagen“ lässt damit einen großen Definitionsspielraum zu und sollte entsprechend konkretisiert werden. Hingewiesen wird an dieser Stelle auch auf den Bayerischen Verfassungsgerichtshof in seiner Entscheidung vom 7. März 2019, Az.: Vf. 15-VII-18, Rn. 74: „Bei der Beurteilung der verfassungsrechtlichen Zulässigkeit von Befugnissen und Maßnahmen, die der Gefahrenab-

wehr dienen, kommt es entscheidend darauf an, welches Gewicht die zu schützenden Rechtsgüter haben. Je gravierender in die grundrechtlich geschützten Positionen der Betroffenen eingegriffen werden kann, umso gewichtiger müssen diese Schutzinteressen sein. Als Grundlage tiefgreifender Maßnahmen kommen grundsätzlich nur besonders gewichtige Rechtsgüter, wie Leib, Leben und Freiheit der Person sowie der Bestand oder die Sicherheit des Bundes oder eines Landes, in Betracht; nicht ausreichend gewichtig kann insoweit ein uneingeschränkter Sachwertschutz sein (vgl. BVerfGE 141, 220 Rn. 108; vom 18.12.2018 – 1 BvR 142/15 – juris Rn. 99)“ (Bayerischer Verfassungsgerichtshof, Entscheidung vom 7. März 2019 – Vf. 15-VII-18 –, Rn. 74, juris).

Der Begriff der Gefahr muss somit hinreichend konkret und als Eingriffsschwelle angesichts der beeinträchtigten Grundrechte hoch genug sein.

Es muss für alle Bürgerinnen und Bürger erkennbar sein, unter welchen Voraussetzungen die Thüringer Polizei Maßnahmen ergreifen darf. Ein normenklares Gesetz schafft auch für die Polizeibeamten Sicherheit in der Anwendung. Diese Möglichkeit sollte der Thüringer Gesetzgeber nutzen.

Die Verfassungsgerichte in Deutschland mussten in jüngster Vergangenheit immer wieder Polizeigesetze rügen, da sie nicht den verfassungsrechtlichen Vorgaben entsprachen, zum Beispiel:

- Bayerischer Verfassungsgerichtshof, Urteil vom 13. März 2025, - Vf. 5-VIII-18, Vf. 7-VII-18, Vf. 10-VIII-18, Vf. 16-VIII-18,
- Bundesverfassungsgericht, Beschluss vom 14.11.2024 - 1 BvL 3/22 - zum Polizeigesetz Nordrhein-Westfalen,
- Bundesverfassungsgericht, Urteil vom 1. Oktober 2024 - 1 BvR 1160/19 - (Bundeskriminalamtgesetz II),
- Verfassungsgerichtshof des Freistaates Sachsen, Urteil vom 25. Januar 2024, - Vf. 91-II-19 - (zum Gesetz zur Neustrukturierung des Polizeirechts des Freistaates Sachsen Sächsischen Polizeigesetz)
- Bundesverfassungsgericht, Urteil vom 16.02.2023 - 1 BvR 1547/19; 1 BvR 2534/20 -,

- Bundesverfassungsgericht, Beschluss vom 9. Dezember 2022 - 1 BvR 1345/21 - (zum Gesetz über die öffentliche Sicherheit und Ordnung in Mecklenburg-Vorpommern),
- Bundesverfassungsgericht, Beschluss vom 27.05.2020 - 1 BvR 1873/13 - (Bestandsdatenauskunft II),
- Bundesverfassungsgericht, Beschluss vom 18. Dezember 2018 - 1 BvR 142/15 - (Kfz-Kennzeichenkontrollen 2) sowie
- Bundesverfassungsgericht, Urteil vom 20.04.2016 - 1 BvR 966/09 -.

Unter einem modernen Polizeigesetz versteht der TLfDI demnach auch die Fähigkeit des Gesetzgebers, Normen zu beschließen, die mit der Verfassung im Einklang stehen.

Um Grundrechtseingriffe abzumildern, können auch etwaige verfahrensrechtliche oder organisatorische Maßnahmen (z.B. Richtervorbehalt) getroffen werden. Auch die Aufnahme einer Befristungsklausel, ggfs. einer wissenschaftlichen Evaluierungspflicht sowie einer Berichtspflicht an den Thüringer Landtag könnten im Gesetz bei einzelnen polizeilichen Maßnahmen verankert werden.

Hingewiesen wird ferner darauf, dass das Gesetz sprachlich dahingehend überprüft werden sollte, ob die Begrifflichkeiten der Richtlinie (EU) 2016/680 (Art. 3), § 32 ThürDSG entsprechen. Es wird in den Überschriften teils von „Datenerhebung“ gesprochen, inhaltlich liegt aber beispielsweise auch eine „Speicherung“ vor. Beide Terminologien fallen unter den Begriff der „Verarbeitung“ (siehe § 32 Nr. 2 ThürDSG).

Abschließend gilt es zu bedenken, dass zwar jede einzelne Maßnahme im Thüringer Polizeiaufgabengesetz begründet erscheinen kann, zusammen können mehrere Maßnahmen aber durchaus das Potenzial entwickeln, zu einem umfangreichen Anwachsen eines Datenbestandes beizutragen, der darüber hinaus auch unter den Voraussetzungen der automatisierten Datenanalyse ausgewertet werden kann. Personenbezogene Daten, die im Rahmen einer Maßnahme verarbeitet

werden, könnten den Ausgangspunkt einer weiteren Maßnahme bilden. Damit bestünde das Risiko einer faktischen Dauererfassung. Zweck des Polizeirechts sollte aber grundsätzlich die Gefahrenabwehr sein, die durch einen möglichst zielgerichteten verfassungsgemäßen Eingriff bewerkstelligt wird.

II. Anmerkungen zum Gesetzentwurf

1. Zu Nr. 4 - § 17 a PAG-E - Meldeauflage:

Die Anordnung der Polizei gegenüber einer Person, sich an bestimmten Tagen zu bestimmten Zeiten bei einer bestimmten Polizeidienststelle zu melden, stellt einen nicht unbedeutenden Grundrechtseingriff dar, der auch das informationelle Selbstbestimmungsrecht tangiert. Daher sollte der Anwendungsbereich eng gehalten werden, zumal die Anordnung dem Bereich der Vorfeldmaßnahme zugeordnet werden kann. Hingewiesen wird an dieser Stelle nochmals auf den Beschluss des Bundesverfassungsgerichts vom 14. November 2024 – 1 BvL 3/22 Rn. 104 ff, juris. Dort hat das Gericht Ausführungen zur Bestimmtheit gemacht und diese in dem dort zugrundeliegenden Sachverhalt bemängelt.

Laut der Gesetzesbegründung (S. 31) soll diese neue PAG-Vorschrift vorrangig im Bereich der Verhütung von Straftaten im Zusammenhang mit Sportereignissen Anwendung finden. Um eine Ausuferung der Anwendungsbereiche einer Meldeauflage zu verhindern, wird angeregt zu prüfen, ob dieser dahingehend noch konkreter festgelegt wird. Die Meldeauflage setzt in § 17a PAG-E keine begangene Straftat voraus, sondern eine Gefahrenprognose, die polizeilich verarbeitet wird.

Aufgenommen wurde nunmehr, dass die Anordnung nur durch den Leiter der zuständigen Polizeibehörde oder durch einen von ihm besonders beauftragten Beamten vorgenommen werden darf. Es wird darauf hingewiesen, dass die Norm in ihrem jetzigen Wortlaut dennoch kein Garant ist, dass ggfs. viele Beamten mit dieser Aufgabe besonders beauftragt werden.

Zu prüfen ist, ob die Verlängerung gerichtlich angeordnet werden muss (siehe hierzu § 52b Abs. 4 Gesetz über die öffentliche Sicherheit und Ordnung in Mecklenburg-Vorpommern).

Fraglich ist, wie in Abs. 3 eine Prüfung der „unzumutbaren Auswirkungen auf die Lebensführung der von der Meldeauflage betroffenen Person“ erfolgen soll. Diese Umstände dürften der Polizei grundsätzlich nicht bekannt sein. Eine Erhebung dieser Umstände auf Vorrat ist aus datenschutzrechtlicher Sicht abzulehnen.

Anzumerken ist, dass die Monatsfrist, sowie deren höchste Verlängerung um einen weiteren Monat missverständlich sein kann. Sofern die Voraussetzungen nach Abs. 1 erneut vorliegen, dürfte ggfs. eine erneute Meldeauflage angeordnet werden. Das Risiko einer dauerhaften Meldeauflage könnte so entstehen.

Selbst wenn die betroffene Person Rechtsschutz ersucht, wird die Maßnahme zunächst vollzogen, da die aufschiebende Wirkung entfällt.

Zu prüfen ist die Aufnahme einer kurzen Speicherfrist von personenbezogenen Daten, die im Rahmen einer solchen Meldeauflage verarbeitet werden.

Schließlich wird darauf hingewiesen, dass mit der Meldeauflage das Risiko besteht, dass die dabei gespeicherten Daten ggf. in Datenanalysen oder Zuverlässigkeitsbewertungen einfließen könnten. Um dies zu vermeiden, wäre ein gesetzlicher Ausschluss einer Weiterverarbeitung zu diesen Zwecken erforderlich.

2. Zu Nr. 6 - § 18a PAG-E - Maßnahmen zum Schutz vor häuslicher Gewalt:

Gemäß § 18a Abs. 3 S. 4 PAG-E übermittelt die Polizei die personenbezogenen Daten der betroffenen Person an eine geeignete Beratungsstelle.

Aus der Begründung zum Gesetzentwurf (S. 32) geht hervor, dass die Teilnahme an einer solchen Beratung die Wahrscheinlichkeit steigern kann, dass „die Polizei zu einem späteren Zeitpunkt gravierende Maßnahmen zur Gefahrenabwehr, wie zum Beispiel die Anwendung unmittelbaren Zwangs oder die Ingewahrsamnahme,

nicht ergreifen muss.“ Die Norm selbst verpflichtet nach ihrem Wortlaut gem. § 18a Abs. 3 S. 3 PAG-E die Polizei, die von der Maßnahme betroffenen Person auf die Möglichkeit der freiwilligen Teilnahme an einer solchen Gewaltpräventionsberatung hinzuweisen. Ob diese Person ein solches Angebot tatsächlich wahrnimmt, obliegt schlussendlich ihr.

Aus datenschutzrechtlicher Sicht ist es nicht erforderlich, bereits proaktiv die personenbezogenen Daten an eine solche Beratungsstelle zu übermitteln, denn zu diesem Zeitpunkt hat niemand Kenntnis darüber, ob die Beratung in Anspruch genommen wird. Kämen darüber hinaus mehrere Beratungsstellen in Betracht, würde eine Datenübermittlung ggf. an mehrere Stellen erfolgen. Aus datenschutzrechtlicher Sicht sollte davon Abstand genommen werden. Es wäre vollkommen ausreichend und datenschutzgerecht, wenn die betroffene Person, die das Angebot annimmt, ihre erforderlichen personenbezogenen Daten im Rahmen des Beratungsangebotes bei der von ihr ausgewählten Stelle selbst angibt. Der § 18a Abs. 3 S. 4 PAG-E sollte aus Sicht des TLfDI gestrichen werden.

Nach § 18a Abs. 4 S. 2 PAG-E übermittelt die Polizei die personenbezogenen Daten der gefährdeten Person an eine geeignete Beratungsstelle. An dieser Stelle gilt das bereits zu § 18a Abs. 3 S. 4 PAG-E Geschriebene. Zwar bezieht sich der Gesetzeswortlaut jetzt nur noch auf eine Stelle („die regional zuständige Interventionsstelle für Opfer häuslicher Gewalt“), die proaktive Übermittlung sollte jedoch aus datenschutzrechtlicher Sicht gestrichen werden. Ob die gefährdete Person sich an die Beratungsstelle wendet, sollte allein ihr obliegen.

3. Zu Nr. 9 - § 21 PAG-E - Behandlung festgehaltener Personen:

Der TLfDI hatte sich bereits in der Vergangenheit zur Schaffung einer gesetzlichen Grundlage für die Videoüberwachung von Gewahrsamsräumen geäußert (siehe dazu 10. Tätigkeitsbericht 2012/2013 S. 127 f.).

§ 21 Abs. 4 und 5 PAG-E enthalten Regelungen zur Bildübertragung (in Form einer Beobachtung und Aufzeichnung) von festgehaltenen Personen, die sich in polizeilichen Gewahrsamseinrichtungen befinden. Der TLfDI geht davon aus, dass hier der einzelne Gewahrsamsraum gemeint ist. Im Rahmen der Bestimmtheit sollte dies in der Norm konkretisiert werden. Tonaufnahmen sind nach dem Wortlaut der Norm ausgeschlossen. Eine Norm muss, um den rechtsstaatlichen Grundsätzen zu genügen, konkret festlegen, unter welchen Voraussetzungen und in welchem Umfang eine solche grundrechtsintensive Maßnahme zulässig ist. Ob dies mit der Formulierung „tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass diese Maßnahme zum Schutz von Personen erforderlich ist“ genügt, ist fraglich. Von hiesiger Seite wird eine Konkretisierung empfohlen (beispielsweise eine Beschränkung auf konkrete Gefahren-/ Notsituationen (körperliche Unversehrtheit, das Leben)). Für andere Überwachungszwecke bedarf es einer weiteren gesetzlichen Grundlage. Der Zweckbindungsgrundsatz muss beachtet werden.

Fraglich ist, ob es beider Regelungen zur Bildübertragung, die sowohl eine Beobachtung als auch eine Aufzeichnungsmöglichkeit zulassen, bedarf. Primäres Ziel ist der Schutz der in Gewahrsam genommenen Person, damit z.B. Suizidversuche oder gesundheitliche Beschwerden erkannt werden können. Um diese Ziele zu erreichen, dürfte in der Vielzahl der Fälle dieser Schutz durch eine reine Beobachtung gewährleistet sein. Eine Bildaufzeichnung wäre zur Gefahrenabwehr insoweit bedeutungslos, da sie gerade nicht dazu beiträgt z.B. bei einem Suizidversuch oder bei Gesundheitsbeeinträchtigungen der in Gewahrsam genommenen Person sofort einzugreifen. Es erfolgt lediglich eine Aufzeichnung. Zudem ist es wahrscheinlich, dass bei dem Bestehen beider Möglichkeiten (Beobachtung und Aufzeichnung) immer auf die vermeintlich sichere Möglichkeit der Aufzeichnung zurückgegriffen wird. Die reine Beobachtung würde somit aller Voraussicht nach in der „Bedeutungslosigkeit“ verschwinden. Sofern dahingehend eingewandt wird, dass die Aufzeichnung auch für eine Rechtmäßigkeitsprüfung der von der polizeilichen Maßnahme betroffenen Person genutzt werden kann, wird darauf hingewiesen, dass das „Ob“ der Videoaufzeichnung im Ermessen der Polizei liegt.

Hinzuweisen ist an dieser Stelle, dass die in Gewahrsam genommene Person keine Möglichkeit hat, sich der Videoüberwachung zu entziehen.

Die Polizei darf zudem nunmehr auch gem. § 21 Abs. 4 S. 2 PAG-E die angefertigten Bildaufzeichnungen automatisch auswerten. Diese Auswertung darf nach dem Wortlaut „[...] nur auf das Erkennen solcher Verhaltensmuster ausgerichtet sein, die auf die Entstehung einer Gefahrensituation für Leben oder Gesundheit der festgehaltenen Person hindeuten“. Durch die Einführung dieser automatischen Auswertung wird eine neue Ebene der Datenverarbeitung erreicht. Es ist fraglich, wie die in der Norm genannten „Verhaltensmuster“ definiert werden. Aufgenommen werden sollte in jedem Fall, dass die automatische Auswertung einer menschlichen Kontrolle bedarf. Die Norm spricht von angefertigten Bildaufzeichnungen. Es stellt sich die Frage, wie mit bereits angefertigten Bildaufzeichnungen, die automatisch ausgewertet werden, Gefahren abgewehrt werden können, oder ob die Aufzeichnungen tatsächlich dann nur den Zweck haben, eine nachträgliche Strafverfolgung zu ermöglichen.

Bevor man die automatische Auswertung in den Gesetzeswortlaut integriert, sollte in Erfahrung gebracht werden, ob diese Technologie überhaupt sicher eine solche Gefahrensituation erkennen kann oder ob sie sehr fehleranfällig und somit falsche Situationen als vermeintliche Gefahr deutet.

Es bleibt schlussendlich sehr fraglich, ob es im Fall einer Videoüberwachung von Gewahrsamsräumen, die lokal und von der Anzahl der Personen, die sich in diesen Räumen befinden, begrenzt ist, einer solchen automatischen Auswertung von Verhaltensmustern überhaupt bedarf (Erforderlichkeit). Der TLfDI spricht sich für eine Streichung der automatischen Auswertung aus.

Die Datenerhebung ist gem. § 21 Abs. 4 S. 4 PAG-E durch ein optisches oder akustisches Signal anzuzeigen. Fraglich ist, ob dieses Signal allein ausreichend ist, damit die Betroffenen wissen, dass nunmehr eine Bildübertragung/Bildaufzeichnung stattfindet. Sie sollten in jedem Fall aktiv darüber informiert werden.

Um den Betroffenen die Möglichkeit zu eröffnen, die Rechtmäßigkeit der polizeilichen Maßnahme überprüfen zu lassen (§ 21 Abs. 5 S. 2 Nr. 2 PAG-E), sollte aufgenommen werden, dass sie auf diese Möglichkeit unverzüglich z.B. nach der Entlassung aus dem Gewahrsam hingewiesen werden müssen, damit sie rechtzeitig vor einer etwaigen Löschung der Aufzeichnungen die Überprüfung einleiten können. In der jetzigen Norm fehlt es an einem solchen Hinweis. Fraglich ist zudem, welche in der Norm genannten „Rechtmäßigkeit“ überprüft werden soll. In Betracht kommen beispielsweise die Rechtmäßigkeit der Videoaufzeichnung an sich oder die Rechtmäßigkeit der polizeilichen Maßnahme in dem Gewahrsamsraum. Dies müsste konkretisiert werden.

Ob es einen Bedarf gibt, die Speicherfrist auf 30 Tage - in Anlehnung an die entsprechenden Regelungen zu Bodycams (§ 33a PAG) - festzulegen, ist fraglich, da beide Bereiche nicht vergleichbar sind.

Nach § 21 Abs. 5 Nr. 1 PAG-E unterbleibt die Löschung der Aufzeichnungen, wenn diese für die Verfolgung von Straftaten benötigt werden. Primäres Ziel der Norm ist die Abwehr einer für die Betroffenen entstehenden Gefahrensituation. Dass diese Aufzeichnungen zur Verfolgung jeglicher Straftaten im Anschluss genutzt werden können, wird von hiesiger Seite kritisch gesehen. Problematisch könnte sein, dass diese Daten auf Vorrat gespeichert werden.

Gem. § 21 Abs. 6 PAG-E können zur Erkennung von Notsituationen technische Mittel zur kontaktlosen Überwachung von Vitalfunktionen eingesetzt werden.

Vitalfunktionen (beispielsweise die Atmung, die Herzfrequenz etc.) zählen zu den besonderen Kategorien personenbezogener Daten gem. § 32 Nr. 14 Buchst. d) ThürDSG. Unklar ist, welche technischen Mittel wie genau zur kontaktlosen Überwachung der Vitalfunktionen eingesetzt werden sollen. Fraglich ist zudem, ob das Personal die erforderlichen Qualifikationen besitzt, Vitalfunktionen überwachen und einschätzen zu können, da es sich dabei regelmäßig nicht um Ärzte handeln dürfte. Regelmäßige Kontrollen durch qualifiziertes Personal könnten hier eine mildere Maßnahme darstellen. Zudem sollte die im Gesetz normierte „Notsituation“ genauer definiert werden.

4. Zu Nr. 14 - § 30a PAG-E - Operativer Opferschutz:

Fraglich ist, ob jegliche Straftat für den operativen Opferschutz in Betracht kommen soll. Gegebenenfalls ist hier eine Konkretisierung vorzunehmen.

Konkretisiert werden sollte weiterhin, unter welchen Voraussetzungen eine Person für die „Schutzmaßnahme geeignet“ ist.

Konkretisiert werden sollte auch, welche Dokumente und Urkunden geändert werden dürfen.

Aufgenommen werden sollten ferner Regelungen, was mit den Daten passiert, wenn die Maßnahme beendet wird und wer darüber benachrichtigt werden muss. Das betrifft auch den Umgang mit den Daten durch die in Abs. 2 genannten Stellen.

5. Zu Nr. 16 - § 33 PAG-E - Datenerhebung bei öffentlichen Veranstaltungen und Ansammlungen sowie an besonderen Orten:

Der TLfDI empfiehlt, die in dieser Norm verwendeten Begrifflichkeiten „Bildaufnahmen, Tonaufnahmen, Bildübertragung, Aufzeichnungen“ zu definieren.

Aufgrund der Zunahme von Übersichtsaufnahmen, die von der Polizei angefertigt werden und die aufgrund der technischen Fortentwicklung zumindest mit einer Personenbeziehbarkeit einhergehen, könnten auch diese in der Norm Berücksichtigung finden.

Durch das Einfügen des Wortes „und“ zwischen der offenen Beobachtung und der Bildaufzeichnung soll der Gesetzeswortlaut zukünftig klarstellen, dass auch eine kumulative Anwendung der Datenerhebung möglich ist. Der TLfDI weist darauf hin, dass eine Beobachtung mittels Bildübertragung grundsätzlich ein milderes Mittel anstelle der Bildaufzeichnung darstellt. Die Beobachtung eines Echtzeitgeschehens, um eine Gefahr abzuwehren, sollte Vorrang vor einer Bildaufzeichnung haben.

Nach § 33 Abs. 4 PAG-E können die angefertigten Bildaufzeichnungen automatisch ausgewertet werden. „Die Auswertung darf dabei nur auf das Erkennen sol-

cher Verhaltensmuster ausgerichtet sein, die auf die Entstehung einer Gefahrensituation oder die Begehung einer Straftat hindeuten.“ Wird ein Verhaltensmuster erkannt, kann eine automatisierte Nachverfolgung des erkannten Störers stattfinden. Nach der Gesetzesbegründung (S. 37) soll damit der Zielvorgabe „modernes Polizeigesetz“ aus dem Regierungsvertrag Rechnung getragen werden.

Mit diesen Erweiterungen erhält die Videoüberwachung durch die Polizei eine neue Dimension, gerade an präsenten und hochfrequentierten Orten, wie dem „Anger“ in Erfurt. Der TLfDI erkennt nicht, dass sich die Polizeiarbeit auch an den technischen Weiterentwicklungen orientieren muss, um eine effektive Gefahrenabwehr zu ermöglichen. Dabei müssen aber auch die Grundrechte der Bürgerinnen und Bürger gewahrt und beachtet werden. Unter Umständen würden die Menschen ihr Verhalten anpassen oder auf ihre Grundrechtsausübung verzichten, wenn sie sich (durch eine Videoüberwachung) beobachtet fühlen (sog. „Chilling-Effect“¹).

Die hier im Gesetzentwurf vorgeschlagene Regelung entwickelt die Videoüberwachung qualitativ weiter. Jetzt steht nicht mehr allein die Befugnis der Polizei zur Videoüberwachung im Raum, sondern mit der Neuregelung wird eine automatische Auswertung dieser Bilddaten geschaffen und eine automatisierte Nachverfolgung von betroffenen Personen ermöglicht. Damit einhergehend ist die Intensivierung des Eingriffs in das Grundrecht auf informationelle Selbstbestimmung einer Vielzahl von Personen, die sich im öffentlichen Raum bewegen und eben keinen Anlass geben, in den Fokus polizeilicher Maßnahmen kommen zu müssen. Die automatische Auswertung und die automatisierte Nachverfolgungsmöglichkeit beziehen sich gem. Abs. 4 zudem auf alle nach § 33 Abs. 1 und Abs. 2 PAG angefertigten Bildaufzeichnungen der dort genannten Orte und Szenarien und beinhalten somit einen großen Anwendungsbereich.

Nach der Begründung des Gesetzentwurfes (S. 37) soll mit der Mustererkennung eine Identifikation von Gefahrensituationen bezweckt werden. Eine Zuordnung potenziell gefährlicher Gegenstände oder Bewegungen zu einer Person soll laut der Gesetzesbegründung (S. 37) nicht stattfinden. Für den TLfDI stellt sich somit

¹ Siehe hierzu „Verhaltensbeeinflussung durch Beobachtung? Eine explorative Nutzerbefragung zu den Auswirkungen verschiedener Beobachtungssituationen“, Nationales Forschungszentrum für angewandte Cybersicherheit ATHENE, 2022, S. 13f abrufbar unter <https://www.jura.uni-frankfurt.de/129979965.pdf>

die Frage, was für die Identifikation einer potenziellen Gefahrensituation herangezogen wird, wenn es nicht eine Bewegung oder ggfs. gefährliche Gegenstände sind. In der Gesetzesbegründung selbst wird im weiteren Verlauf von „auffällige Bewegungsmuster aufspüren“ und „abstrakte Bewegungsmuster“ gesprochen. Festzustellen ist jedoch, dass das System Gefahrensituationen erkennt und damit zumindest implizit ein Verhalten bewertet.

Hingewiesen wird darüber hinaus auch auf die Fehleranfälligkeit solcher Systeme. Unter Umständen wird dann z. B. eine Umarmung fälschlicherweise als Schlag gedeutet oder als potenzielle Erdrösselung von dem System identifiziert. Somit könnten unbescholtene Personen von (weiteren) polizeilichen Maßnahmen in Anspruch genommen werden, die nur aufgrund eines technischen-funktionellen Fehlers als potentielle Störer identifiziert wurden. Die Bewertungsmaßstäbe bleiben hier hinlänglich intransparent. Erschwerend kommt hinzu, dass diese Auswertung unbemerkt erfolgt und sich die betroffenen Personen nicht dagegen wehren können. Es erfolgt eine Verhaltensanalyse von Personen im öffentlichen Raum. Bevor eine solche Regelung aufgenommen wird, sollte zumindest eruiert werden, ob diese Systeme überhaupt ihren vermeintlichen Nutzen erfüllen. Dabei können Erfahrungen auch aus anderen Bundesländern hilfreich sein.

Die in Abs. 4 aufgenommene Möglichkeit der automatisierten Nachverfolgung soll laut der Gesetzesbegründung (S. 37) anhand einer von der Künstlichen Intelligenz gestützten Funktion stattfinden. In unübersichtlichen Lagen wird der vermeintliche grundrechtsschonende Zwischenschritt der Prüfung einer Gefahrensituation durch einen Polizeibeamten aller Wahrscheinlichkeit nach kurz ausfallen und die automatisierte Nachverfolgung somit eventuell ziemlich schnell in Anspruch genommen. Durch die Nachverfolgung könnten ggfs. auch Bewegungsprofile entstehen. Damit wiederum könnten ggfs. etwaige Verhaltenszusammenhänge hergestellt werden. Fraglich ist, welcher retrograde Aufzeichnungszeitraum ausgewertet und nachverfolgt werden darf. Da die Nachverfolgung potenziell alle Personen betreffen kann, sieht der TLfDI einen nicht unerheblichen Grundrechtseingriff.

Hingewiesen wird an dieser Stelle darauf, dass mit der Einführung des § 38 PAG-E auch Drohnen für die Datenerhebung nach § 33 Abs. 1 PAG (bei öffentlichen Veranstaltungen und Ansammlungen) eingesetzt werden dürfen, was im Zusam-

menspiel mit der Auswertungs- und Nachverfolgungsmöglichkeit eine neue Qualität der Polizeiarbeit erreicht.

Der TLfDI lehnt die Ausweitung der automatischen Auswertung und der automatisierten Nachverfolgung in der geplanten Form ab und spricht sich für eine Streichung der Regelung aus.

Zu § 33 Abs. 3 PAG regt der TLfDI an, die Aufbewahrungsfrist unter der Berücksichtigung des Datenminimierungsgrundsatzes von derzeit einem Monat zu kürzen (siehe z.B. § 15a Abs. 2 PolNRW). Je länger die Aufbewahrungsfristen sind, desto mehr verlagert sich der eigentliche Zweck der polizeilichen Maßnahme (Gefahrenabwehr) zu einer Verfolgungsmaßnahme von Straftaten oder Ordnungswidrigkeiten von erheblicher Bedeutung.

Unter Bezugnahme auf das Urteil des Sächsischen Verfassungsgerichtshofes vom 25. Januar 2024 (Az.: Vf 91-II-19, Rn. 368ff, juris.) wird angeregt, auch § 33 Abs. 2 Nr. 2 PAG-E einer verfassungsrechtlichen Überprüfung im Hinblick auf die Bestimmtheit und Normenklarheit zu unterziehen.

6. Zu Nr. 17 - § 33b PAG-E - Datenerhebung bei Notrufen, Aufzeichnung von Notrufen:

Aus der Gesetzesbegründung (S. 38) geht hervor, dass der standardisierte Dienst „Advanced Mobile Location (AML)“ zum Einsatz kommen soll. Die Ortung mittels AML ist grundsätzlich geeignet, Leben zu retten. Die Angabe des Ortes durch den Notanrufenden selbst ist oft ungenau oder ggfs. sogar unmöglich. Dennoch muss jede Verarbeitung dieser Daten in einem engen zeitlichen und zweckgebundenen Rahmen beschränkt bleiben. Der jetzige Wortlaut „[...] alle durch einen Anbieter von Telekommunikationsdiensten im Rahmen einer Notrufverbindung übermittelten oder zum Abruf bereitgestellten personenbezogenen Daten [...]“ ist sehr weit gefasst. Hier sollte eine klare Begrenzung auf die erforderlichen Daten erfolgen. Es sollte aus datenschutzrechtlicher Sicht demnach sichergestellt werden, dass nur diese Daten erhoben werden, die für den Notrufeinsatz unbedingt erforderlich sind. Die Daten sollten zudem ausschließlich für die Abwicklung des Notfalleinsatz-

zes verarbeitet werden dürfen. Empfohlen wird daher eine nur sehr kurze Speicherung mit anschließender Löschung der Daten. Eine dauerhafte Verarbeitung für die Aufgabenerfüllung der Polizei, ohne dass ein konkreter Notfallbezug besteht, wäre unverhältnismäßig.

Zu bedenken ist, dass mit der neuen Formulierung auch Daten aus Video- und Textnotrufen erhoben werden. Dies ist weiter als die bisherige Datenerhebung. Fraglich ist, ob es tatsächlich dieser erweiterten Datenerhebung bedarf.

Auch in diesem Zusammenhang wird erneut darauf hingewiesen, dass die aufgrund dieser Norm erhobenen Daten ggf. in eine Datenanalyse einfließen könnten. Fraglich ist, ob dies gewollt ist.

7. Zu Nr. 18 - § 33c PAG-E - Automatisierte Kraftfahrzeugkennzeichenerkennung:

Die Neuregelung soll die Rechtsprechung des Bundesverfassungsgerichts (Urteil vom 11. März 2008 1 BvR 2074/05 und Beschluss vom 18. Dezember 2018, 1 BvR 142/15) umsetzen. Das Bundesverfassungsgericht stellt in seinem Beschluss vom 18. Dezember 2018 fest, dass die automatisierte Kraftfahrzeugkennzeichenkontrolle bereits mit der Erfassung der Nummernschilder, auch wenn das Ergebnis zu einem Nichttreffer führt und die Daten sogleich gelöscht werden, einen Eingriff in das informationelle Selbstbestimmungsrecht darstellt. (BVerfG, Beschluss vom 18.12.2018 1 BvR 142/15 1. Leitsatz, juris). Verfassungsrechtlich nicht ausgeschlossen hat das Gericht aber Rechtsgrundlagen, die einen solchen Eingriff zulassen. Diese müssen aber den Anforderungen an die Verhältnismäßigkeit entsprechen. Gleichwohl wird eine Vielzahl von unbeteiligten Personen durch die Maßnahme erfasst.

In § 33c PAG-E kann eine automatisierte Kraftfahrzeugkennzeichenerkennung unter den Voraussetzungen des § 14 Abs. 1 Nr. 1 - 6 PAG (Identitätsfeststellung), mit Einschränkungen in § 33c Abs. 1 Nr. 1 und Nr. 2 PAG-E, vorgenommen werden. Vor dem Hintergrund, dass es sich bei der automatisierten Kraftfahrzeug-

kennzeichenerkennung um eine eingriffsintensive Maßnahme handelt, die auch Daten von einer Vielzahl von Personen einbezieht, bei denen letztendlich keine Treffer festgestellt werden, sollte dennoch geprüft werden, ob die in § 14 Abs. 1 Nr. 1 - 6 PAG genannten Voraussetzungen hinreichend bestimmt sind.

In das Gesetz sollte aufgenommen werden, dass der Abgleich nur mit vollständigen Kennzeichen des Fahndungsbestandes durchgeführt werden darf (siehe hierzu auch § 51 Abs. 2 S. 4 Polizeigesetz Baden-Württemberg).

Konkretisiert werden sollte auch der Fahndungsbestand, der erstellt wurde über Personen, die zum Zweck der Durchführung ausländerrechtlicher Maßnahmen ausgeschrieben sind. Dieser lässt in der derzeitigen Fassung einen weiten Abgleichbestand zu. Aufgrund der Erfassung einer Vielzahl von Kennzeichen sollten die Fahndungsbestände streng begrenzt werden.

§ 33c Abs.1 Satz 5 PAG-E regelt, dass „die automatisierte Kraftfahrzeugkennzeichenerkennung nicht flächendeckend und nicht dauerhaft durchgeführt werden“ darf. Aufgenommen werden sollte ferner der Zusatz, dass der Einsatz der technischen Mittel „weder einzeln noch in der Kombination“ erfolgt (siehe hierzu § 58 Abs. 2 Satz 1 und 2 Sächsisches Polizeivollzugsdienstgesetz (SächsPVDG)).

Zudem sollte im Gesetzentwurf ergänzt werden, dass die Maßnahme offen zu erfolgen hat und in geeigneter Weise darauf hinzuweisen ist (vgl. § 58 Abs. 2 Satz 2 SächsPVDG).

8. Zu Nr. 19 - § 34 PAG-E - Besondere Mittel der Datenerhebung:

Der TLfDI verweist in diesem Zusammenhang auf den Beschluss des Bundesverfassungsgerichts vom 14. November 2024, Az. 1 BvL 3/22. Die längerfristige Observation unter Anfertigung von Bildaufnahmen und Bildaufzeichnungen begründen einen schweren Eingriff in das informationelle Selbstbestimmungsrecht. „Die verfassungsrechtliche Rechtfertigung der Datenerhebung durch heimliche Überwachungsmaßnahmen mit hoher Eingriffsintensität im Bereich der Gefahrenabwehr verlangt als Eingriffsschwelle entweder eine konkrete Gefahr oder eine wenigstens konkretisierte Gefahr. Es muss gewährleistet sein, dass eine Gefährdung

der durch die Norm geschützten 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.“ (BVerfG, Beschluss vom 14.11.2024, Az. 1 BvL 3/22, 2. Leitsatz, juris).

Der TLfDI regt an, diese Norm dahingehend zu überprüfen, ob sie den vom Bundesverfassungsgericht gesetzten Voraussetzungen entspricht. In der Begründung zum Gesetzentwurf (S. 39) werden im Rahmen des Schutzgutes der kritischen Infrastruktur Anlagen, wie die öffentliche Verwaltung, Schulen, Ärztezentren oder Serverzentren als davon umfasst angehen. Es wird darauf hingewiesen, dass der Anwendungsbereich damit ziemlich weit gefasst wird, um dann mit den in der Norm genannten besonderen Mitteln eine verdeckte Datenerhebung durchzuführen, die insbesondere auch unbeteiligte Dritte erfassen kann (siehe hierzu auch das Urteil des BVerfG vom 26. April 2022 – 1 BvR 1619/17, Rn. 243, das ein enges Verständnis beim Schutz von Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, verlangt). Hier bedarf es einer Konkretisierung, insbesondere der genannten „öffentlicher Verwaltung“, sofern sie überhaupt darunterfallen sollte.

Bezüglich der in § 34 Abs. 1 Nr. 2 PAG genannten Person wird auf das Urteil des Bundesverfassungsgerichts verwiesen, das sich mit der heimlichen Überwachung etwaiger Kontaktpersonen auseinandersetzt (BVerfG, Urteil vom 1. Oktober 2024 – 1 BvR 1160/19 Rn. 96ff., juris). Dies ist zwar im vorliegenden Entwurf nicht Teil der Änderung, es sollte dennoch überprüft werden, ob es den verfassungsrechtlichen Anforderungen entspricht.

Bei § 34 Abs. 4 S. 3 PAG-E wird empfohlen, „drei Werktage“ in die Formulierung „drei Tage“ abzuändern. Ansonsten könnte die Maßnahme unter Umständen einen viel längeren Zeitraum erfassen, wenn sie z.B. am Wochenende erfolgt.

Auch in diesem Zusammenhang ist fraglich, ob die aufgrund dieser Norm erhobenen Daten ggf. in eine Datenanalyse einfließen könnten.

9. Zu Nr. 20 - § 34a PAG-E - Überwachung der Telekommunikation:

Auch hier wird der Sachgüterschutz wie in § 34 PAG-E angepasst auf „[...] Anlagen der kritischen Infrastruktur oder sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen [...]“. Die von hiesiger Seite dazu unter § 34 PAG-E gemachten Ausführungen gelten entsprechend.

10. Zu Nr. 21 - § 34b PAG-E - Erhebung von Telekommunikationsverkehrsdaten und Nutzungsdaten:

Auch hier wird der Sachgüterschutz wie in § 34 PAG-E angepasst auf „[...] Anlagen der kritischen Infrastruktur oder sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen [...]“. Die von hiesiger Seite dazu unter § 34 PAG-E gemachten Ausführungen gelten entsprechend.

11. Zu Nr. 22 - § 34c PAG-E - Identifizierung und Lokalisierung von Mobilfunkkarten und -endgeräten:

In § 34c Abs. 1 PAG-E wird der Sachgüterschutz wie in § 34 PAG-E angepasst auf „[...] Anlagen der kritischen Infrastruktur oder sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen [...]“. Die von hiesiger Seite dazu unter § 34 PAG-E gemachten Ausführungen gelten entsprechend.

Eingefügt wird in § 34c Abs. 1 Nr. 2 PAG-E die Aufnahme von „vermissten, suizidgefährdeten oder hilflosen Personen“. Der Kreis der betroffenen Personen wird damit erweitert. Diese Personengruppen sollten konkretisiert werden. Unter Umständen befindet sich die vermisste Person in keiner hilflosen Lage, sondern möchte nicht aufgefunden werden.

Weiterhin sollte der Aufbau der Vorschrift überarbeitet werden. In der jetzigen Fassung kann nach dem Wortlaut der Norm der Standort von vermissten, suizid-

gefährdeten oder hilflosen Personen ermittelt werden zur Abwehr einer Gefahr für den Bestand oder die Sicherheit der Bundesrepublik Deutschland oder zur Abwehr einer Gefahr für Anlagen der kritischen Infrastruktur oder sonstigen Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen. Jedoch dürfte bei diesen Fällen (vermisste, suizidgefährdete oder hilflose Personen) eine Ermittlung des Standorts eines Mobilfunkendgeräts lediglich bei einer Gefahr für deren Leben, Gesundheit oder Freiheit in Betracht kommen. Im Sinne der Normenklarheit wird hier eine redaktionelle Anpassung empfohlen.

Aufgenommen werden sollten ferner Vorgaben zur Häufigkeit der Standortermittlung. Ein Fehlen dieser Vorgaben hatte der Sächsische Verfassungsgerichtshof in seiner Entscheidung vom 25. Januar 2024 kritisiert (siehe Urteil Sächsischer Verfassungsgerichtshof 25.01.2024 – Vf 91-II-19, Rn. 219ff, juris).

12. Zu Nr. 23 - § 34e PAG-E - Erhebung von Bestandsdaten:

Mit der Änderung soll die bisher auf Bestandsdaten der Telekommunikation beschränkte Regelung auf Bestandsdaten digitaler Dienste erweitert werden. Laut der Gesetzesbegründung (S. 40) erfolgt dies, weil die digitalen Dienste in den letzten Jahren zunehmend an Bedeutung gewonnen und die klassischen Formen der Telekommunikation fast verdrängt haben. Digitale Dienste sind elektronische Informations- und Kommunikationsdienste, aber auch eine große Anzahl an Internetdiensten (siehe hierzu

<https://www.bfdi.bund.de/DE/Buerger/Inhalte/Telemedien/Telemedien.html>).

Seitens des TLfDI wird darauf hingewiesen, dass die Aussagekraft über eine Person bei digitalen Diensten in der heutigen Zeit wohl wesentlich stärker sein wird, als bei Telefondaten. Der Anwendungsbereich wird damit deutlich erweitert.

§ 34e Abs. 1 PAG-E enthält die einfache Bestandsdatenabfrage, erweitert auf die digitalen Dienste. Laut Gesetzesbegründung (S. 40) ist diese beim Vorliegen einer konkreten Gefahr zulässig. Das Vorliegen einer konkreten Gefahr sollte im Gesetzeswortlaut ergänzt werden.

§ 34e Abs. 2 PAG-E regelt die polizeiliche Anfrage einer IP-Adresse und sieht dabei gesteigerte Tatbestandvoraussetzungen vor.

§ 34e Abs. 3 PAG-E enthält nunmehr auch die Befugnis zur Auskunftserlangung von Passwörtern und Zugangssicherungs-codes auf Endgeräte und Speichereinrichtungen. Diese Befugnis steht grundsätzlich unter einem Richtervorbehalt. Auskunftsverlangen nach Passwörtern und Zugangssicherungs-codes beinhalten einen sehr intensiven Eingriff in das Recht auf informationelle Selbstbestimmung. Diese Zugangsdaten können besonders missbrauchsanfällig sein. Die dadurch geschützten Informationen können unter Umständen sensible Bereiche des Lebens nicht nur der Person selbst, sondern auch Informationen von Dritten betreffen. Es ist zu prüfen, ob weitere Regelungen zur Sicherung dieser Daten in den Gesetzeswortlaut aufgenommen werden müssen, beispielsweise, dass sie gegen unbefugte Kenntnisnahme und Verarbeitung besonders zu sichern sind.

Noch klarer sollte aufgenommen werden, dass mit der Erlangung von Passwörtern und Zugangssicherungs-codes nicht automatisch sämtliche Inhalte erlangt werden dürfen.

Nach § 34e Abs. 4 S. 4 PAG-E ist die richterliche Anordnung obsolet, wenn der Betroffene vom Auskunftsverlangen bereits Kenntnis hat oder haben muss. Durch diesen Passus besteht die Gefahr, dass der grundsätzliche Richtervorbehalt umgangen werden könnte. Hier wäre zu prüfen, ob dieser Satz gestrichen werden sollte.

Auch in diesem Zusammenhang ist fraglich, ob die aufgrund dieser Norm erhobenen Daten ggf. in eine Datenanalyse einfließen könnten.

13. Zu Nr. 24 - § 34f PAG-E - Datenerhebung durch verdeckt handelnde Personen:

In § 34f Abs. 2 Nr. 1 - 3 PAG-E erfolgt die Aufzählung der verdeckt handelnden Personen. Fraglich ist, ob es einer richterlichen Anordnung auch für den Einsatz des nicht offen ermittelnden Polizeibeamten bedarf.

Die Anordnung der Maßnahme ist nach dem Gesetzentwurf unzulässig, wenn „tatsächliche Anhaltspunkte für die Annahme vorliegen, dass durch die Maßnahme mit hoher Wahrscheinlichkeit Kenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt würden“. Zu prüfen ist, ob eine „hohe Wahrscheinlichkeit“ vorliegen muss oder nicht bereits eine „Wahrscheinlichkeit“ ausreichend ist, um die Maßnahme nicht durchzuführen.

In § 34f Abs. 3 PAG-E wird festgelegt, dass die verdeckt handelnde Person vor jeder Weitergabe von Informationen eigenständig zu prüfen hat, ob durch die Informationen oder die Art und Weise, wie sie erlangt wurden, der Kernbereich privater Lebensgestaltung der überwachten Person berührt ist. Fraglich ist, ob eine Vertrauensperson, die möglicherweise keine tiefergehenden Kenntnisse zu dieser Thematik besitzt, diese Anforderung erfüllen kann und auch bereit dazu ist.

Aufgenommen werden sollte zudem, dass es keine doppelte Führung etwaiger Vertrauenspersonen bei der Polizei und dem Verfassungsschutz geben darf (Trennungsgebot von Polizei und Verfassungsschutz (siehe dazu Jahn, Gazeas, Hübner, StV 2023, Seite 417.)).

Nach § 34f Abs. 6 PAG-E ist die Vertrauensperson fortlaufend auf ihre Zuverlässigkeit zu überprüfen. Fraglich ist, wie diese Zuverlässigkeitsüberprüfung vorgenommen wird. Hier sollte die Norm entsprechend konkretisiert werden.

Hingewiesen wird an dieser Stelle, dass auf Bundesebene in der 20. Wahlperiode ein umfangreicher Entwurf eines Gesetzes zu jeweils einzelnen Regelungen des Einsatzes von verdeckten Ermittlern und Vertrauenspersonen sowie zur Tatprovokation von der Bundesregierung (Drs. 20/11312) eingebracht wurde. Dieser hatte sich durch den Ablauf der Wahlperiode erledigt

(<https://dip.bundestag.de/vorgang/gesetz-zur-regelung-des-einsatzes-von-verdeckten-ermittlern-und-vertrauenspersonen/309832>).

14. Zu Nr. 24 - § 34g PAG-E - Elektronische Aufenthaltsüberwachung:

Die elektronische Aufenthaltsüberwachung stellt einen schwerwiegenden Eingriff in das informationelle Selbstbestimmungsrecht der überwachten Person dar.

Es bestehen Zweifel, ob tatsächlich durch die elektronische Aufenthaltsüberwachung ein Präventionszweck erzielt werden kann und es damit ein geeignetes Mittel darstellt. Insoweit liegen dem TLfDI auch keine wissenschaftlichen Erkenntnisse vor. Diese sollten jedoch einer Begründung zugrunde liegen.

Das Bundesverfassungsgericht bestätigte zwar im Rahmen seiner Entscheidung vom 01. Dezember 2020, Az. 2 BvR 916/11, dass die elektronische Aufenthaltsüberwachung verurteilter Personen im Rahmen der Führungsaufsicht verfassungsgemäß sei. Gleichzeitig verwies es aber auf eine im Auftrag des Bundesministeriums der Justiz und für Verbraucherschutz vorgenommene Evaluierung, wonach eine gesicherte Schlussfolgerung zur Wirksamkeit der elektronischen Aufenthaltsüberwachung im Hinblick auf die Rückfallhäufigkeit nicht möglich sei. Es seien jedoch zum Teil erhebliche Einschränkungen festzustellen, von denen einige potentiell die Resozialisierung beeinträchtigen könnten, so z.B. berufliche Schwierigkeiten, körperliche Beschwerden, Vermeidung bestimmter Orte (über etwaige Gebots- oder Verbotszonen hinaus) aus Angst vor Stigmatisierung, Schwierigkeiten bei der Wohnungssuche (siehe ausführlicher BVerfG vom 01.12.2020, Az. 2 BvR 916/11 zitiert nach juris, Rn.175 und 177).

Mit der vorliegenden Normierung der elektronischen Aufenthaltsüberwachung im PAG-E ist es möglich, eine betroffene Person einer dauerhaften Überwachung, inklusive einer Standorterfassung zu unterwerfen. Die dadurch ermöglichte potenzielle Erstellung eines Bewegungsprofils kann Rückschlüsse auf dessen gesamte Lebensführung ziehen. Auch eine Drittbetroffenheit ist nicht auszuschließen. Zudem dürfen die dabei erhobenen Daten auch zweckändernd verarbeitet werden.

Der vorliegende Gesetzentwurf definiert in § 34g Abs. 1 Nr. 1 - 4 PAG-E, in welchen Fällen eine elektronische Aufenthaltsüberwachung durchgeführt werden kann. Fraglich ist, ob der Gesetzgeber tatsächlich bei allen dort aufgeführten Fällen eine solche Maßnahme gewollt hat. Durch die gewählte Formulierung in Nr. 1

ist der Anwendungsbereich sehr weit gefasst, weil lediglich eine Gefahr für bestimmte Rechtsgüter vorliegen und die Maßnahme dafür zwingend erforderlich sein muss. Fälle, die eigentlich unter die speziellen Voraussetzungen von Nr. 2 fallen, könnten unter Umständen dann bereits unter Nr. 1 (Leben, Gesundheit oder Freiheit einer Person) subsumiert werden. Daher sollte Nr. 1 unbedingt konkretisiert werden. Im Zusammenspiel mit § 34g Abs. 3 Nr. 1 PAG-E, der eine Datenverarbeitung zur Verfolgung von Straftaten gegen die in Abs. 1 Nr. 1 genannten Rechtsgüter zulässt, wirkt diese Maßnahme sehr weitreichend.

In § 34g Abs. 1 Nr. 2 PAG-E sollte das Tatbestandsmerkmal „übersehbarer Zeitraum“ konkreter gefasst werden. Zu prüfen ist zudem, ob die Straftatbestände der §§ 224, 226 StGB ggfs. vergleichsweise zu niederschwellig sind, um die Maßnahme zu rechtfertigen. Nach der Begründung des Gesetzentwurfs (S. 43) dient der § 34g Abs. 1 Nr. 2 PAG-E für die Überwachung rückfallgefährdeter Sexualstraftäter. Es könnte an einem ausreichend konkreten Zusammenhang zwischen diesem Normzweck und jenem der §§ 224, 226 StGB (anders als z.B. bei den ebenfalls in Abs. 1 Nr. 2 aufgeführten §§ 176 ff. (wobei § 176c StGB wiederum nicht aufgenommen wurde) oder 182 StGB) fehlen.

In § 34g Abs. 1 Nr. 3 PAG-E ist fraglich, ob der Begriff „in absehbarer Zeit“ näher bestimmt werden sollte.

In § 34g Abs. 2 PAG-E sollten die Fälle ausdrücklich normiert werden, wann einer gefährdeten Person ein solches technisches Mittel zur Verfügung gestellt wird. Fraglich ist, ab welchem Radius ein Signal an die gefährdete Person geschickt wird.

Klarstellend sollte in § 34g Abs. 3 PAG-E aufgenommen werden, dass mit den Daten keine allgemeinen Bewegungsanalysen durchgeführt werden dürfen.

Gemäß § 34g Abs. 3 S. 2 PAG-E dürfen innerhalb einer Wohnung keine über den Umstand der Anwesenheit der betroffenen Person hinausgehenden Aufenthaltsdaten erhoben werden. Zu prüfen ist, ob zusätzlich klarstellend aufgenommen

werden muss, dass dennoch erhobene Daten nicht verwendet werden dürfen und unverzüglich zu löschen sind.

Laut der Gesetzesbegründung (S. 44) dürfen die Daten gem. § 34g Abs. 3 S. 3 Nr. 2 PAG-E auch zu anderen, in Nr. 2 genannten Gefahrenabwehrlagen genutzt werden. Dies sollte konkretisiert werden.

Nach § 34g Abs. 3 S. 2 Nr. 4 PAG-E dürfen Daten verarbeitet werden zur Aufrechterhaltung der Funktionsfähigkeit des technischen Mittels. Der Empfang von Ortsdaten beweist technisch immer, dass das Gerät noch funktionsfähig ist. Damit können aufgrund von § 34g Abs. 3 S. 2 Nr. 4 PAG-E beliebige Ortsdaten erhoben werden, da Nr. 4 immer zutrifft. Sofern sich Nr. 4 auf eine „Beeinträchtigung der Datenerhebung“ bezieht (z.B. niedriger Batteriestand, schlechter Empfang), wird empfohlen, § 34g Abs. 3 S. 2 Nr. 4 PAG-E auch nur auf diese Art der Daten zu beziehen. Die momentane Formulierung würde es zulassen, Ortsdaten zur Aufrechterhaltung der Funktionsfähigkeit zu speichern.

Fraglich ist, ob § 34g Abs. 5 PAG-E – wie in der Entwurfsbegründung geschrieben – vom Schrankenvorbehalt des Art. 13 Abs. 7 GG gedeckt ist. Laut der Begründung des Gesetzentwurfs (S. 44) geht es um die Befugnis der Polizei, die Wohnung des Betroffenen zur Aufstellung einer Heimeinheit (sog. „Home Unit“) betreten zu dürfen. Gemäß Art. 13 Abs. 7 GG dürfen Eingriffe und Beschränkungen nur zur Abwehr einer gemeinen Gefahr oder einer Lebensgefahr für einzelne Personen, auf Grund eines Gesetzes auch zur Verhütung dringender Gefahren für die öffentliche Sicherheit und Ordnung vorgenommen werden.

Nach § 34g Abs. 5 S. 2 PAG-E hat die betroffene Person auf Aufforderung die technischen Mittel an die Polizei unverzüglich herauszugeben. Da nach § 34g Abs. 2 PAG-E die gefährdete Person auch ein technisches Mittel zur Verfügung gestellt bekommen soll, das die Annäherung der verantwortlichen Person signalisiert, sollte auch hier die Rückgabe des technischen Mittels normiert werden.

Sofern die Maßnahme im PAG verankert wird, ist zu prüfen, ob eine Befristungsklausel und eine Evaluierungsklausel (wie z.B. in § 34c PolG NRW, § 61 Abs. 8 SächsPVDG bezüglich Evaluierungsklausel) aufgenommen werden sollten. Gleich-

ches gilt hinsichtlich einer jährlichen Unterrichtung des Landtags durch die Landesregierung (§ 34c Abs. 10 PolG NRW, § 61 Abs. 8 SächsPVDG).

Angemerkt wird, dass sich der TLfDI gemäß § 112 Abs. 4 der Geschäftsordnung des Thüringer Landtags bereits zu dieser Thematik im Rahmen des „Zweiten Gesetz zur Änderung des Polizeiaufgabengesetzes - Verhinderung von Gewalt gegen Frauen und häuslicher Gewalt -Drucksache 7/9652-“ kritisch geäußert hatte.

15. Zu Nr. 25 - § 35 PAG-E - Wohnraumüberwachung:

§ 35 Abs. 3 PAG-E erlaubt, dass Maßnahmen der Wohnraumüberwachung auch in Wohnungen anderer Personen unter den dort aufgeführten Bestimmungen zulässig sind. Die Norm orientiert sich dabei am Wortlaut des § 46 Abs. 2 des Bundeskriminalamtgesetzes. Auch wenn die Gesetzesbegründung (S. 45) von einer „behutsamen“ Erweiterung spricht, ist dies ein schwerwiegender Eingriff in Grundrechte von unbeteiligten dritten Personen in deren Wohnungen. Eine Gefahr von diesen dritten Personen geht gerade nicht aus. Durch die Maßnahme können dennoch ihre privaten Lebenssachverhalte erfasst werden.

§ 35 Abs. 3 Nr. 2 PAG-E sollte dahingehend konkretisiert werden, was unter der Formulierung „allein nicht zur Abwehr der Gefahr“ zu verstehen ist. Fraglich ist, welche Kriterien dafür erfüllt sein müssen (z.B. zur Ermittlung des Aufenthaltsortes). Zudem sollte der klarstellende Zusatz aufgenommen werden, dass die Maßnahme in Wohnungen von Dritten nur angewandt werden darf, wenn die Gefahr auf andere Weise nicht abgewehrt werden kann.

16. Zu Nr. 26 - § 36 PAG-E - Gemeinsame Verfahrensbestimmungen für Maßnahmen der verdeckten Datenerhebung:

Hingewiesen wird, dass es zu Auslegungsschwierigkeiten kommen kann bei den in § 36 Nr. 1 und Nr. 2 PAG erwähnten „erheblich mitbetroffenen Personen“. Empfehlenswert ist hier eine Konkretisierung.

17. Zu Nr. 27 - § 37 PAG-E - Ausschreibung zur polizeilichen Beobachtung, zur Ermittlungsanfrage und zur gezielten Kontrolle:

Mit den Änderungen in § 37 PAG-E sollen die Vorgaben des Bundesverfassungsgerichts aus seinem Beschluss (Bundesverfassungsgericht, Beschluss vom 09.12.2022- 1 BvR 1345/21 - zum Sicherheits- und Ordnungsgesetz - SOG M-V) umgesetzt werden. Hinzuweisen ist an dieser Stelle, dass sich auch der Verfassungsgerichtshof des Freistaates Sachsen am 25. Januar 2024 zur Ausschreibung zur polizeilichen Beobachtung und Kontrolle geäußert hat und diese als nicht vereinbar mit Art. 33 SächsVerf gesehen hat. Gerügt wurde in diesem Verfahren die Verletzung des Übermaßgebotes, weil es am Erfordernis einer konkretisierten Gefahr fehlte (siehe Urteil Sächsischer Verfassungsgerichtshof 25.01.2024 – Vf 91-II-19, S. 251ff., juris.).

Nach § 37 Abs. 2 Nr. 1 PAG-E ist eine Ausschreibung zulässig, wenn „die Gesamtwürdigung einer Person und ihrer bisher begangenen Straftaten erwarten lässt, dass sie auch künftig besonders schwere Straftaten begehen wird [...]“ Dies lässt einen eher weiten Prognosespielraum offen und sollte deshalb konkretisiert werden. Fraglich ist, welche Qualität und Quantität die bisher begangenen Straftaten haben müssen (z.B.: müssen sie gleichartig sein?, wie lange dürfen die Straftaten zurückliegen, um berücksichtigt zu werden?). Fraglich ist auch, welche weiteren Tatsachen bei der Person vorliegen müssen, um in die „Gesamtwürdigung“ einzufließen.

Selbiges gilt für § 37 Abs. 2 Nr. 2 PAG-E. Fraglich ist, was unter einem „individuelle[n] Verhalten“ verstanden werden soll und was als „überschaubarer Zeitraum“ definiert wird.

Bei § 37 Abs. 2 Nr. 1 und Nr. 2 PAG-E führt die Gesetzesbegründung (S. 46) zu den besonders schweren Straftaten aus, dass „[...] grundsätzlich solche, die mit einer Höchststrafe von mehr als fünf Jahren bedroht sind.“, darunterfallen. Um dem Bestimmtheitsgebot zu genügen, wird eine Konkretisierung empfohlen.

Zu eruieren ist, ob wie in § 47 Abs. 4 BKAG eine Überprüfungsfrist nach sechs Monaten, deren Dokumentation sowie eine richterliche Anordnung bei Verlängerung der Maßnahme, aufgenommen werden soll.

18. Zu Nr. 28 - § 38 - Einsatz von unbemannten Luftfahrtsystemen:

Die Nutzung von Drohnen eröffnet der Polizei ein größeres Potenzial im Rahmen ihrer Überwachungsmöglichkeiten. Eine Drohne kann größere Menschenmengen erfassen und ermöglicht einen schnellen Positionswechsel. Gleichzeitig ist sie aber deutlich weniger erkennbar als beispielsweise ein klassischer Videowagen der Polizei. Positiv ist deshalb die Aufnahme im Entwurf dieses Gesetzes, dass auch beim Einsatz von Drohnen die Offenkundigkeit der Maßnahme gewahrt werden muss. Gem. § 38 Abs. 2 S. 2 PAG-E „soll“ jedoch lediglich auf das unbemannte Luftfahrtsystem hingewiesen werden. Der TLfDI spricht sich für die Streichung der „Soll-Vorschrift“ aus und empfiehlt die Verpflichtung zum Hinweis. In der Praxis wird zukünftig trotzdem das Problem bestehen, wie die Polizei diese Offenheit umsetzt.

Nach § 38 Abs. 1 Nr. 1 PAG-E dürfen unbemannte Luftfahrtsysteme als Plattform für eine Datenerhebung bei öffentlichen Veranstaltungen und Ansammlungen nach § 33 Abs. 1 PAG eingesetzt werden. In Kombination mit den neuen Maßnahmen der Mustererkennung und der Nachverfolgungsmöglichkeit, kann die Videoüberwachung mittels Drohnen im Rahmen von § 33 Abs. 1 PAG damit ein neues, flächendeckendes System der Überwachung erreichen. Hingewiesen wird hier auf die Ausführungen zu § 33 PAG-E.

Kritisch ist aus datenschutzrechtlicher Sicht auch § 38 Abs. 1 Nr. 2 PAG-E zu sehen. Es erlaubt die Verwendung der Drohnen als besonderes Mittel der Datenerhebung. Das würde beispielsweise bedeuten, dass auch eine längerfristige Observation mittels Drohne durchgeführt werden kann.

Fraglich ist, ob bei § 38 Abs. 1 Nr. 3 PAG-E (Identifizierung und Lokalisierung von Mobilfunkkarten und -endgeräten) die Nutzung einer Drohne für das Auffinden des für die Gefahr Verantwortlichen erforderlich ist oder ob mit einem Einsatz einer Drohne nur die Ortung vermisster, suizidgefährdeten oder hilflosen Personen bezweckt werden soll.

19. Zu Nr. 28 - § 39 PAG-E - Zweckbindung, hypothetische Datenneuerhebung und Kennzeichnung von Daten:

a) Vorbemerkung:

Der Grundsatz der hypothetischen Datenneuerhebung besagt, dass eine zweckändernde Nutzung von personenbezogenen Daten, die durch eingriffsintensive Maßnahmen erhoben wurden, nur dann zulässig ist, wenn ihre Neuerhebung für den geänderten Zweck nach verfassungsrechtlichen Maßstäben mit vergleichbar schwerwiegenden Mitteln erfolgen dürfte (BVerfGE 141, 220 (327 f.)). Ein wichtiger Anwendungsfall dieser zweckändernden Nutzung ist die Datenübermittlung an andere Sicherheitsbehörden (BVerfGE 154, 152 (266 f.); 156, 11 (49f.); 162, 1 (108f.), 163, 43 (Rn. 122 ff.); BVerfG Beschluss vom 17.07.2024, 1 BvR 2133/22, Rn. 101 ff., siehe dazu Löffelmann, Hypothetische Datenneuerhebung und konkrete Schutzkategorien – ein kohärentes Datenverarbeitungskonzept für die Sicherheitsbehörden von Bund und Ländern, GSZ 2024, S. 215 ff).

Die Bestimmungen in § 39 Abs. 1 bis 3 PAG-E, die z. B. mit § 20 Abs. 1 bis 3 des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG) weitestgehend übereinstimmen, übernehmen die Vorgaben und Formulierungen aus der Entscheidung des BVerfG zum BKAG 1997 (BVerfGE 141, 220-378, siehe oben).

Indem die (Bundes- und Landes-) Gesetzgeber die an sie gerichteten verfassungsrechtlichen Anforderungen an die Formulierung der Normen über die Daten(weiter)verarbeitung nahezu unverändert in die Bundes- bzw. Landesnormen übernommen haben, statt sie als Maßstab für ihre eigene Normsetzung heranzuziehen, verlagern sie die Verantwortung für einen verfassungskonformen Umgang mit personenbezogenen Daten auf die Exekutive - hier also die Polizei – und entledigen sich damit ihrer Pflicht zur Schaffung hinreichend bestimmter Handlungs Vorgaben für die Polizeibeamten (siehe zu dieser Kritik: BeckOK PolR Hessen/Bäuerle, 34. Ed. 25.2.2025, HSOG § 20, Rn. 36). Diese Vorgehensweise des TMIKL ist hier vom TLfDI zu kritisieren, weil die Landesregierung damit das Risiko einer rechtswidrigen Datenverarbeitung unnötig auf die Polizei und ihre Beamtinnen und Beamte abwälzt. Dabei gibt es durchaus systematische Ansätze zur Bildung miteinander korrespondierender Kategorien des Daten- und des Rechtsgüterschutzes (siehe dazu Löffelmann, a.a.O., S. 215 ff.).

Diese Ausführungen sind auch als Antwort auf die Frage 90 des Fragenkatalogs zum vorliegenden PAG-Entwurf zu verstehen.

b) Zu § 39 Abs. 2 Nr. 2 b) PAG-E:

Als Tatbestandsvoraussetzung für die Datenweiterarbeitung zu anderen Zwecken bestimmt § 39 Abs. 2 Nr. 2 b) PAG-E, „wenn sich im Einzelfall konkrete Ermittlungsansätze zur Abwehr von in einem übersehbaren Zeitraum drohenden Gefahren für mindestens vergleichbar bedeutsame Rechtsgüter erkennen lassen.“

Mit diesem Tatbestandsmerkmal übernimmt nun auch die Thüringer Landesregierung eine Formulierung, die das BVerfG als abgesenkte Eingriffsschwelle bisher nur für die Abwehr terroristischer Gefahren akzeptiert hat (BVerfG NJW 2016, 1781, Rn 164). Die generalisierende Übernahme dieser Formulierung in die Zweckänderungsregelung nach dem Grundsatz der hypothetischen Datenneuerhebung für die Abwehr jedweder drohenden Gefahr für vergleichbare Rechtsgüter dürfte daher den verfassungsrechtlichen Anforderungen kaum genügen (so für die Hessische Regelung in § 20 Abs. 2

Nr. 2 b) HSOG: BeckOK PolR Hessen/Bäuerle, 34. Ed. 25.2.2025, HSOG § 20, Rn. 74-75).

Der TLfDI rät daher zur entsprechenden Änderung des § 39 Abs. 2 Nr. 2 b) PAG-E.

c) Zu § 39 Abs. 6 PAG-E:

§ 39 Abs. 6 PAG-E nimmt Bezug auf § 39 Abs. 5 PAG-E. In letztgenannter Regelung ist bestimmt, wie und welche Zusatzinformationen (Mittel, Kategorie, Rechtsgüter, Straftaten und erhebende Stellen) für die Beachtung und Einhaltung des Grundsatzes der hypothetischen Datenneuerhebung zu kennzeichnen sind. Wenn nun aber in § 39 Abs. 6 PAG-E bestimmt ist, dass zum einen die Regelung des § 39 Abs. 5 PAG-E nicht gilt, soweit eine Kennzeichnung tatsächlich nicht möglich ist, und zum anderen die Regelung des § 39 Abs. 5 PAG-E auch bis zum 31. Dezember 2032 nicht gelten soll, soweit eine Kennzeichnung aus technischen Gründen nicht möglich ist, so wird mit der Regelung des § 39 Abs. 6 PAG-E eine wesentliche Voraussetzung des Grundsatzes der hypothetischen Neuerhebung - die Kennzeichnungspflicht der erhobenen Daten – außer Kraft gesetzt. Diese viel zu weitreichende Ausnahmeregelung ist sowohl aus verfassungsrechtlichen als auch aus datenschutzrechtlichen Gründen abzulehnen!

Wenn – wie es in der Gesetzesbegründung zu § 39 Abs. 6 PAG-E überdies anklingt, dass § 39 Abs. 6 Satz 1 PAG-E für Altdaten gelten soll, bei denen nicht bekannt oder feststellbar ist, wer sie erhoben hat oder zu welchen Zwecken sie ursprünglich erhoben worden sind - dann kann und sollte diese Determinierung auch so in den Gesetzestext aufgenommen werden (und nicht nur in der für den Anwender nicht leicht verfügbaren Gesetzesbegründung enthalten sein).

Diese Ausführungen sind auch als Antwort auf die Fragen 91 und 92 des Fragenkatalogs zum vorliegenden PAG-Entwurf zu verstehen.

20. Zu Nr. 29 - § 40 PAG-E - Weiterverarbeitung von Daten:

a) Vorbemerkung:

Der TLfDI erlaubt sich auch zu dieser Norm eine Vorbemerkung systematischer Art: Wenn in den drei Änderungsbefehlen zur bereits bestehenden Norm des § 40 PAG jeweils auf den Regelungsgehalt des § 39 PAG-E verwiesen wird, stellt sich die berechnigte Frage, warum die Landesregierung hier nicht die Regelungszwecke des § 39 PAG-E UND des neuen § 40 PAG-E in EINER Norm zusammengefasst hat. Dies wäre für die Polizistin bzw. den Polizisten in der Praxis sicherlich anwendungsfreundlicher. Zudem wären dabei vielleicht auch die folgenden Widersprüche zwischen den beiden Normen aufgefallen.

b) Zu § 40 Abs. 1 PAG-E:

Aus Sicht des TLfDI sind die Verarbeitungszwecke des § 39 Abs. 1 und 2 PAG-E nicht kompatibel mit jenen des (jetzigen) § 40 Abs. 1 PAG - und werden es auch nicht durch die vorgesehene Ergänzung in § 40 PAG (Nr. 29 a) des vorliegenden Gesetzentwurfs. Denn während § 39 Abs. 1 und Abs. 2 PAG-E eine Weiterverarbeitung von personenbezogenen Daten nur für die konkrete Vorgangsverarbeitung gem. § 39 Abs. 1 PAG-E oder für eine verfahrensübergreifende Verwendung nach § 39 Abs. 2 PAG-E - sofern dafür im Einzelfall konkrete Ermittlungsansätze vorliegen – gestattet § 40 Abs. 1 PAG in seiner jetzigen Fassung eine Weiterverarbeitung von personenbezogenen Daten unter anderem zu einer zeitlich befristeten Dokumentation oder zur (allgemeinen) Vorgangsverwaltung. Diese unterschiedlichen Regelungszwecke sind aus der Sicht des TLfDI nicht miteinander vereinbar. Dies gilt umso mehr dadurch, dass es sich bei Vorgangsverwaltung und befristeter Dokumentation um der Polizei zustehende Annexkompetenzen handelt (so Ebert/Joel/Krämer, Thüringer Gesetz über die Aufgaben und Befugnisse der Polizei, 9. Auflage, § 40, Rn. 17).

c) Zu § 40 Abs. 2 PAG-E:

Auch die Regelungszwecke des § 40 Abs. 2 PAG-E sind nicht vereinbar mit jenen des § 39 Abs. 2 Nr. 2 PAG-E: Denn die Befugnis zur Weiterverarbeitung personenbezogener Daten im Anwendungsbereich des bereits geltenden § 40 Abs. 2 PAG dient der Gefahrenabwehr, insbesondere der vorbeugenden Bekämpfung von Straftaten. Demgegenüber erfordert die Befugnis zur Weiterverarbeitung personenbezogener Daten zu anderen Zwecken, als zu denen sie erhoben worden sind gem. § 39 Abs. 2 Nr. 2 PAG-E ein „Mehr“, nämlich das Vorliegen von „im Einzelfall konkrete[n] Ermittlungsansätzen“.

Des Weiteren ist in diesem Zusammenhang auf die Zweifel auch des TLfDI hinzuweisen, ob die bisherige Regelung des § 40 Abs. 2 PAG den Vorgaben des Bundesverfassungsgerichts zur vorsorgenden Speicherung genügt (siehe hierzu BVerfG, 1. Senat, 1 BvR 1160/19 vom 01.10.2024, Bundeskriminalamtgesetz II, Rn. 180 bis 191 der juris-Entscheidung). In der genannten Entscheidung verlangen die Richter und Richterinnen für eine vorsorgende Speicherung als Zweckänderung vier konkrete Parameter, nämlich (1.) eine eindeutig erkennbare Zweckbestimmung, (2.) konkrete Anforderungen an die Eingriffsschwellen in Form von Speicherschwellen, (3.) spezifische Begrenzungen zur Speicherdauer sowie (4.) klare Verwendungsregeln und differenzierte organisatorische und verfahrensrechtliche Anforderungen sowie adäquate Kontrollmöglichkeiten. Insbesondere an den konkreten Vorgaben für eine Speicherschwelle leidet die Regelung in § 40 Abs. 2 PAG aus der Sicht des TLfDI. Wichtig wäre es, als Erfordernis eine sog. (Negativ-)Prognose zu verlangen (das BVerfG führt dazu Folgendes aus: *„Als taugliche Prognosekriterien können insbesondere die Art, Schwere und Begehungsweise der vormaligen Tat sowie die Persönlichkeit des Betroffenen und sein bisheriges strafrechtliches Erscheinungsbild in Frage kommen. Von Bedeutung wird angesichts der allgemeinen fachwissenschaftlichen Erkenntnisse zu Kriminalprognosen regelmäßig sein, ob die Person wiederholt und in welchem Ausmaß sie straffällig geworden ist“* (BVerfG, a.a.O., Rn. 186 der juris-Entscheidung).

Diese Ausführungen sind auch als Antwort auf die Fragen 94 des Fragenkatalogs zum vorliegenden PAG-Entwurf zu verstehen.

d) Zu § 40 Abs. 3 PAG-E:

Ebenso wie bei § 40 Abs. 1 und 2 PAG sind auch bei § 40 Abs. 3 PAG dessen Regelungszwecke nicht mit denen des § 39 Abs. 1 und Abs. 2 PAG-E vereinbar. Denn die Speicherung von personenbezogenen Daten des in § 40 Abs. 3 PAG genannten Personenkreises (Zeugen, Opfer einer künftigen Straftat sowie Verbindungspersonen zu Verurteilten, Beschuldigten oder Verdächtigen einer Straftat) erfolgt weder (nur) zur Erfüllung derselben Aufgabe gem. § 39 Abs. 1 Nr. 1 PAG-E oder (nur) zum Schutz derselben Rechtsgüter oder derselben Straftaten gem. § 39 Abs. 1 Nr. 2 PAG-E noch zur Verfolgung konkreter Ermittlungsansätze gem. § 39 Abs. 2 Nr. 2 PAG-E.

Diese Ausführungen sind auch als Antwort auf die Frage 96 des Fragenkatalogs zum vorliegenden PAG-Entwurf zu verstehen.

e) Zu § 40 Abs. 6 PAG:

Der TLfDI spricht sich erneut (siehe zur Kritik bereits den 10. Tätigkeitsbericht des TLfDI zum Datenschutz, Öffentlicher Bereich, Nrn. 7.7 und 7.8 sowie den 11. Tätigkeitsbericht des TLfDI, Öffentlicher Bereich, Nr. 7.11) dafür aus, die sogenannte „Mitziehklausel“ zu streichen. Diese besagt, dass, soweit innerhalb der Speicherrfrist für ein Ereignis – aufgrund eines neuen Ereignisses – eine weitere Speicherung hinzukommt, das für den neuen Fall berechnete Prüfdatum bzw. diese Prüffrist (aus § 40 Abs. 6 ThürPAG in Verbindung mit ThürPolPrüffristVO) für die gesamte Speicherung maßgeblich wird; es kommt damit zum einem „Neustart“ der jeweiligen Prüffrist. Aufgrund der neuen Speicherung unterfallen weiter zurückliegende Ereignisse letztendlich der festgesetzten neuen Prüffrist. Vor dem Hintergrund, dass der PAG-E neue polizeiliche Maßnahmen vorsieht und damit einhergehend die Datenmenge quantitativ weiter steigen wird, wäre dies auch ein proba-

tes Mittel, den polizeilichen Datenbestand auf ein grundrechtsschonendes Mindestmaß zu reduzieren.

Gleichzeitig wird ganz grundsätzlich empfohlen, die Fristen der polizeilichen Datenspeicherung einer genauen Überprüfung unterziehen und ggfs. zu kürzen.

Insgesamt ist daher die Regelung des § 40 PAG in seiner angestrebten Neufassung komplett zu überarbeiten.

21. Zu Nr. 30 - § 40a PAG-E - Anlassbezogene automatisierte Datenanalyse:

a) Vorbemerkung:

Mit der Einfügung von § 40 a PAG-E in das PAG ebnet die Landesregierung die Einführung des sog. „**Data-mining**“ in den Befugniskanon der Thüringer Polizei. Dieses „Data-mining“ liegt nach einer Definition der Bundesregierung immer dann vor, wenn Verfahren und Methoden eingesetzt werden, „mit deren Hilfe bereits vorhandene große Datenbestände, zumeist auf statistisch-mathematischen Verfahren basierend, selbständig auf Zusammenhänge analysiert werden, um auf diesem Wege ‚neues Wissen‘ zu generieren“ (Antwort der Bundesregierung auf eine Kleine Anfrage BT-Drs. 17/11582, 3, in Bezug genommen auch vom BVerfG ZD 202, 205 Rn. 74; siehe dazu BeckOK Polizei- und Ordnungsrecht Hessen, Möst/Bäuerle, 34. Edition, § 25a HSOG, Rn. 26.1).

Unbedingt zu beachten und als Prüfungsmaßstab für den § 40a PAG-E zu Grunde zu legen ist das Urteil des Bundesverfassungsgerichts vom 16.02.2023 (1 BvR 1547/19, 1 BvR 2634/20), in dem die Karlsruher Richter sowohl die damalige Hessische Regelung als auch die Hamburgische Norm zur automatisierten Datenanalyse für nichtig erklärt hatten.

Der TLfDI erkennt nicht, dass die Landesregierung in ihrem Gesetzentwurf bemüht war, die Vorgaben aus dem genannten BVerfG-Urteil bei der Regelung der

Voraussetzungen für eine anlassbezogene automatisierte Datenanalyse gem. § 40a PAG-E möglichst weit zu beachten und umzusetzen. Dennoch dürfte die vorliegende Regelung des § 40a PAG-E – insbesondere in ihren Absätzen 1 und 2 – den Bestimmtheitsgesichtspunkten bei Eingriffsnormen nicht (vollständig) genügen, da die für Bürgerinnen und Bürger erforderliche Vorhersehbarkeit von der mit der Regelung verbundenen Eingriffen in ihr Recht auf informationelle Selbstbestimmung hier nicht erreicht wird.

b) Zu § 40a Abs. 1 PAG-E:

Da § 40a Abs. 1 Satz 1 PAG-E auf die Voraussetzungen des § 39 PAG-E verweist, ist hier auch noch einmal auf die Anmerkungen und Änderungsvorschläge des TLfDI zu § 39 PAG-E hinzuweisen (siehe oben unter Nr. 19 dieser Stellungnahme).

Voraussetzung für die automatisierte Zusammenführung von gespeicherten personenbezogenen Daten ist nach § 40a Abs. 1 Satz 1 PAG-E das Vorliegen einer **Gefahr** für den Bestand oder die Sicherheit der Bundesrepublik Deutschland oder eines Landes, für Leben, Gesundheit oder Freiheit einer Person oder zur Abwehr einer **Gefahr** für Anlagen der kritischen Infrastruktur oder sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen.

Aus der Begründung zu § 40a PAG-E ist zu entnehmen, dass es sich jeweils um eine **konkrete Gefahr** handeln muss. Unter Berücksichtigung des Urteils des ThürVerfGH vom 21.11.2012 (VerfGH 19/09) hält es der TLfDI daher für erforderlich, bereits im Gesetzestext des § 40a Abs. 1 Satz 1 PAG-E den Begriff der „konkreten Gefahr“ zu verwenden. Denn auch im darauffolgenden Satz – in § 40a Abs. 1 Satz 2 PAG-E – wird der Begriff der dringenden Gefahr konkret benannt und verwendet.

Diese Ausführungen sind auch als Antwort auf die Frage 101 des Fragenkatalogs zum vorliegenden PAG-Entwurf zu verstehen.

Schließlich ist im Rahmen der Bewertung des Wortlauts von § 40a Abs. 1 Satz 1 PAG-E noch einmal darauf hinzuweisen, dass es nicht nur jedem Bürger bzw. jeder Bürgerin schwerfallen dürfte, zu erahnen, welche Gebäude oder sonstige Einrichtungen unter „Anlagen der kritischen Infrastruktur“ sowie unter „Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen“ zu subsumieren sind. Im Sinne der Normenklarheit bzw. Bestimmtheit einer Norm wären hier Konkretisierungen wünschenswert.

c) Zu § 40a Abs. 2 PAG-E:

In § 40a Abs. 2 PAG-E wird in dessen Satz 3 bestimmt, dass für die Anordnung von Maßnahmen nach § 40a Abs. 2 Satz 1 PAG-E der § 34 Absatz 5 PAG entsprechend gilt. Danach darf also der Leiter der Landespolizeidirektion oder der Leiter des Landeskriminalamtes oder ein von diesen besonders beauftragter Beamter des höheren Polizeivollzugsdienstes diese Maßnahmen anordnen. Im Hinblick auf die Eingriffsschwere, noch dazu weit im Vorfeld von Straftaten, und die Vielzahl der verarbeiteten personenbezogenen Daten hält der TLfDI hier die Anordnung durch einen Richter / eine Richterin für erforderlich.

Diese Ausführungen sind auch als Antwort auf die Frage 104 des Fragenkatalogs zum vorliegenden PAG-Entwurf zu verstehen.

Fraglich ist zudem, inwieweit auch **Verkehrsdaten aus Funkzellenabfragen** hier in den Kreis der für eine anlassbezogene automatisierte Datenanalyse ausgeschlossenen Daten nach § 40a Abs. 2 Satz 2 PAG-E aufgenommen werden sollten. Das BVerfG thematisiert diese Frage in seinem Urteil vom 16.02.2023 (1 BvR 1547/19, 1 BvR 2634/20 Rn. 142 der juris-Entscheidung). Dies sollte – wie bereits in der Stellungnahme des TLfDI zur Kabinettanhörung dargelegt – einer Prüfung unterzogen werden.

Diese Ausführungen sind auch als Antwort auf die Frage 103 des Fragenkatalogs zum vorliegenden PAG-Entwurf zu verstehen.

d) Zu § 40a Abs. 3 PAG-E:

Der Wortlaut des § 40a Abs. 3 PAG-E ist in der vorliegenden Fassung viel zu unbestimmt, da aus ihm nicht klar für die Rechtsanwender hervorgeht, welche personenbezogenen Daten aus welchen Systemen konkret in die Datenanalyse einfließen. Diese wäre auf jeden Fall näher gesetzlich zu normieren.

Diese Ausführungen sind auch als Antwort auf die Frage 98 des Fragenkatalogs zum vorliegenden PAG-Entwurf zu verstehen.

e) Zu § 40a Abs. 4 PAG-E:

In § 40a Abs. 4 PAG-E ist in dessen Satz 1 die Auswahl und Schulung des eingesetzten Personals geregelt, und in Satz 2 dieses Norm-Entwurfs ist Folgendes bestimmt: „Durch technische und organisatorische Maßnahmen sind die Zugriffsmöglichkeiten des eingesetzten Personals auf die zur Verfügung stehenden personenbezogenen Daten auf das erforderliche Maß zu beschränken.“

Demgegenüber hat das Bundesverfassungsgericht in seiner Entscheidung vom 16.02.2023 (a.a.O., Rn. 140 der juris-Entscheidung) Folgendes ausgeführt: *„Die allgemeinen Datenschutzregelungen in § 20 Abs. 4 HSOG und § 66 HDSG und in § 56 Hmb-PolDVG verpflichten zwar zu organisatorischen und technischen Vorkehrungen, die die Einhaltung der Zweckbindung sicherstellen. Hierdurch wird der Zugriff auf Daten für eine automatisierte Datenanalyse und -auswertung aber nicht hinreichend normenklar und bestimmt eingeschränkt. Dies müsste – jedenfalls mit Blick auf die Befugnis aus § 25a HSOG und § 49 Hmb-PolDVG – näher geregelt werden. Technisch-organisatorische Sicherungen, die die Einhaltung der Zweckbindung sicherstellen, können etwa in der technischen Trennung von Datenbeständen nach unterschiedlichen Verarbeitungszwecken **oder einer zweckabhän-***

*gigen Verteilung von Zugriffsrechten auf Datenbestände bestehen [...]. Die hessische Landesregierung hat mehrfach dargelegt, dass nach einem speziellen Rollen- und Rechtskonzept in unterschiedlichem Ausmaß Zugriff auf die Analyseplattform gestattet werde [...]. **Ein solches Konzept kann im Grundsatz zu einer technisch-organisatorischen Sicherung der Zweckbindung geeignet sein, ist aber bislang nicht normiert. Der Gesetzgeber hat hierzu keine Vorgaben gemacht [...]. Die angegriffenen Vorschriften selbst regeln dies jedoch nicht und ermächtigen und verpflichten auch die Verwaltung nicht zur Erstellung eines solchen Konzepts. Die Verwaltung hat in Hessen zwar ihr spezielles Rollen- und Rechtskonzept entwickelt und geht nach diesem vor, hat dies bislang jedoch nicht als abstrakt generelle Regelung in einer öffentlich zugänglichen Weise dokumentiert.***

Erst aufgrund dieser Vorgaben des Bundesverfassungsgerichts ist in Hessen der § 25a Abs. 3 Satz 2 und 3 des HSOG dergestalt geändert worden, dass dort nun das Vorhandensein eines Rollen- und Rechtskonzepts sowie eines Konzepts der Kategorisierung und Kennzeichnung personenbezogener Daten in einer **Verwaltungsvorschrift** geregelt ist. Diese Konzepte orientieren sich an dem übergeordneten Ziel der Reduzierung des jeweils zu analysierenden Datenvolumens, der Angemessenheit der jeweils angewandten Analysemethode und des größtmöglichen Schutzes Unbeteiligter (funktionale Reduzierung der Eingriffsintensität). Das **Rollen- und Rechtskonzept** gem. § 25a Abs. 3 Nr. 1 HSOG regelt dabei die zweckabhängige Verteilung sachlich eingeschränkter Zugriffsrechte anhand von Phänomenbereichen. Maßstab dafür sind das Gewicht der zu schützenden Rechtsgüter und der Grad der Dringlichkeit des polizeilichen Einschreitens. Es ist nach dem Prinzip auszugestalten, wonach mehr Berechtigte Zugriff auf weniger und wenige Berechtigte Zugriff auf mehr der in der Analyseplattform zusammengeführten Daten haben dürfen. Es müssen darin mindestens die einzelnen Phänomenbereiche, ihre Gewichtung und ihr Verhältnis zueinander umschrieben und die dienstrechtliche Stellung der Berechtigten, ihre Funktion und ihre spezifische Qualifizierung bezogen auf den Umfang der jeweiligen Berechtigung festgelegt werden.

Diese Verwaltungsvorschrift zur Ausführung des § 25a HSOG vom 12.07.2023 (StAnz. 2023, S. 946) hat diese gesetzlichen Vorgaben übernommen.

Für § 40a Abs. 4 Satz 2 PAG-E ergibt sich daraus, dass die wenigen Einschränkungen (Beschränkung der Zugriffsmöglichkeiten des eingesetzten Personals, Beschränkung auf das erforderliche Maß) den verfassungsgerichtlichen Vorgaben aus dem Urteil vom 16.02.2023 **nicht im Ansatz gerecht** werden dürften. Der TLfDI empfiehlt daher, hier eine Regelung dahingehend zu ergänzen, die den Hessischen Ansatz übernimmt.

f) Fehlen der Zugriffskontrolle und der ständigen Protokollierung sowie Anhörung des Landesbeauftragten für den Datenschutz und die Informationsfreiheit

Keine Regelungen trifft der PAG-Gesetzentwurf (und auch keine andere Regelung des PAGs) zur Zugriffskontrolle und zur Protokollierung der Zugriff der anlassbezogenen automatisierten Datenanalyse. Deshalb sollten entsprechende Vorgaben, die z. B. § 25a Abs. 4 HSOG dazu trifft, in § 40a PAG-E hinsichtlich der Zugriffskontrolle und der ständigen Protokollierung ergänzt werden.

Zudem weist der TLfDI darauf hin, dass der Hessische Beauftragte für den Datenschutz und die Informationsfreiheit gem. § 25a Abs. 5 HSOG vor der Einrichtung oder einer wesentlichen Änderung einer automatisierten Anwendung zur Datenanalyse anzuhören, wobei diese Anhörung bei Gefahr im Verzug nachzuholen ist.

Diese Ausführungen sind auch als Antwort auf die Frage 97 des Fragenkatalogs zum vorliegenden PAG-Entwurf zu verstehen.

22. Zu Nr. 34 - § 43a PAG-E - Nachträglicher biometrischer Abgleich mit öffentlich frei zugänglichen personenbezogenen Daten aus dem Internet:

Die Regelung erlaubt den nachträglichen Abgleich biometrischer Daten zu Gesichtern und Stimmen mit öffentlich zugänglichen Daten aus dem Internet mittels einer automatisierten Anwendung zur Datenverarbeitung. Das Bundesverfassungsgericht hatte bereits in seinem Urteil zur Kraftfahrzeugkennzeichenerfassung festgestellt, dass die Erhebung personenbezogener Daten, auch wenn sie öffentlich zugänglich sein sollten, einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung darstellt (BVerfG, Beschluss vom 18.12.2018 - 1 BvR 142/15 - Rn. 39, juris: „Auch entfällt der grundrechtliche Schutz nicht schon deshalb, weil die betroffene Information öffentlich zugänglich ist. Auch wenn der Einzelne sich in die Öffentlichkeit begibt, schützt das Recht auf informationelle Selbstbestimmung dessen Interesse, dass die damit verbundenen personenbezogenen Informationen nicht im Zuge automatisierter Informationserhebung zur Speicherung mit der Möglichkeit der Weiterverwertung erfasst werden (vgl. BVerfGE 120, 378 <399>)“).

Die Intensität hängt insbesondere von der Art der ausgewerteten Daten, der eingesetzten Technik und dem Grad der Automatisierung ab (siehe hierzu auch Entschließung der Datenschutzkonferenz vom 20. September 2024, abrufbar unter https://www.datenschutzkonferenz-online.de/media/en/2024-09-20_Entschliessung_DSK_Gesichtserkennung.pdf).

Die gesetzliche Grundlage, die diesen Eingriff gestattet, muss insbesondere hinreichend bestimmt und verhältnismäßig sein. Da mit der vorliegenden Maßnahme ein erheblicher Grundrechtseingriff einhergeht, steigen die Anforderungen an die gesetzliche Norm. Zu berücksichtigen ist, dass ein Abgleich mit öffentlich zugänglichen Daten einen nicht unerheblichen Anteil von Menschen erfasst, die anlasslos und unbemerkt mitüberwacht und in die Maßnahme einbezogen werden (siehe Dr. Stephan Schindler, Universität Kassel, Stellungnahme zur öffentlichen Anhörung zu den Gesetzentwürfen der Fraktionen SPD, BÜNDNIS 90/DIE GRÜNEN und FDP „Entwurf eines Gesetzes zur Verbesserung der inneren Sicherheit und des Asylsystems“ (BT-Drs. 20/12805) und „Entwurf eines Gesetzes zur Verbesserung der Terrorismusbekämpfung“ (BT-Drs. 20/12806) sowie der Gesetzentwurf der

Fraktion der CDU/CSU „Entwurf eines Gesetzes zur Begrenzung des illegalen Zustroms von Drittstaatsangehörigen nach Deutschland (Zustrombegrenzungs-gesetz)“ (BT-Drs. 20/12804 vom 22.09.2024, S. 3)).

Auch hier besteht die Gefahr des „chilling effects“ in der Form, dass Personen ihr Verhalten ändern bzw. sich in ihrer öffentlichen Kommunikation zurückziehen, wenn sie dadurch in den Fokus staatlicher Maßnahmen gelangen könnten (siehe Dr. Stephan Schindler, a.a.O., S. 3, der damit einhergehend auch eine Einschränkung des Grundrechts auf Meinungsfreiheit sieht). Aufgrund der Vielzahl der Bilder, die Menschen im Internet von sich selbst veröffentlichen oder die von Dritten veröffentlicht werden, ohne dass die Person davon Kenntnis erlangt (beispielsweise als Beifang auf einem Bild, unrechtmäßige Veröffentlichung), können Rückschlüsse auf ihr komplettes Leben gezogen werden (siehe hierzu Dr. Stephan Schindler, a.a.O., S. 4, 11). Dies könnte die Möglichkeit eröffnen, ein umfassendes Lebensprofil von einer Person zu erstellen.

Nicht zu unterschätzen ist zudem auch hier wieder die mögliche Fehleranfälligkeit des technischen Systems. Aufgrund eines technisch fehlerhaften Abgleichs könnten Menschen von der staatlichen Maßnahme erfasst und im Nachhinein irrtümlich durch weitere polizeiliche Handlungen in Anspruch genommen werden (so auch Dr. Stephan Schindler, a.a.O., S. 3).

Nach § 43a Abs. 1 PAG-E darf die „Polizei alle öffentlich frei zugänglichen personenbezogenen biometrischen Daten aus dem Internet erheben und diese nachträglich mit biometrischen Daten zu Gesichtern und Stimmen, die sie für die Erfüllung ihrer Aufgaben weiterverarbeitet oder für die sie eine Berechtigung zum Abruf hat, mittels einer automatisierten Anwendung zur Datenverarbeitung abgleichen [...]“. Fraglich ist in diesem Zusammenhang, was unter dem Begriff „Abgleich“ in Bezug zum Zweck der Vorschrift zu verstehen ist. Nach dem Wortlaut ist ein Abgleich zur Identifizierung oder Ermittlung eines Aufenthaltsortes der für die Gefahr verantwortlichen Person oder für die Abwehr von Gefahren der in der Norm genannten Rechtsgüter zulässig. Dies ist sehr weitgehend, da die Maßnahme somit in einer Vielzahl von Fällen Anwendung finden kann. Angesichts der Tragweite

und der Eingriffsintensität dieser Maßnahme ist die Einschränkung des Anwendungsbereichs dringend geboten.

Im Moment besteht die Gefahr eines fast routinemäßigen Internetabgleichs, ohne dass eine Beschränkung auf eine Zielperson erfolgt. Es erfolgt auch keine weitere Prüfung, ob die Maßnahme nicht außer Verhältnis zur Bedeutung des Sachverhalts steht. Somit betrifft die Regelung eine große Anzahl von Personen, die mit ihren öffentlich zugänglichen personenbezogenen Daten im Internet sind. All jene werden in einen Abgleich einbezogen – das Internet und die darin enthaltenen personenbezogenen Daten zu Gesichtern und Stimmen dienen damit als riesige Referenzdatenbank.

Da der Abgleich automatisiert erfolgt, ist es möglich, innerhalb eines kurzen Zeitraums eine Unmenge an Daten von einer großen Anzahl an Menschen aus der gesamten Bevölkerung in einen Datenabgleich einzubeziehen. Dies erhöht die Tragweite der Maßnahme umso mehr. Zu Bedenken ist, dass die in § 43a Abs.1 S. 1 PAG-E genannten Daten zu Gesichtern und Stimmen aus dem Internet nicht per se biometrische Daten sind. Gem. § 32 Nr. 12 ThürDSG sind „biometrische Daten mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen [...]“. Das bedeutet, dass erst durch ein technisches Verfahren biometrische Daten zu einer Person hergestellt werden können. Der Wortlaut ist insoweit zumindest missverständlich.

Der TLfDI geht davon aus, dass im Rahmen von § 43a PAG-E ein KI-System zum Einsatz kommt. Die aus dem Internet erhobenen Daten müssten dabei wohl zumindest kurzzeitig auf einer Datenbank hinterlegt werden, um dann einen Abgleich zu ermöglichen. Insofern ist fraglich, ob der Wortlaut in § 43a Abs. 1 PAG-E, der nur von „Erheben“ spricht, die tatsächlich beabsichtigte Datenverarbeitung abbildet.

Gem. Art. 6 Abs. 2 in Verbindung mit Anhang III Nr. 1a) KI-Verordnung (EU) 2024/1689 (KI-VO) gelten biometrische Fernidentifizierungssysteme (Definition in Art. 3 Nr. 41 der KI-VO) als Hochrisiko-Systeme. Art. 5 Abs. 1 lit. e) KI-VO verbie-

tet das ungezielte Auslesen von Gesichtsbildern aus dem Internet. Fraglich ist, ob hier ein gezieltes oder ungezieltes Auslesen erfolgen soll. Der Wortlaut in § 43a Abs. 1 PAG-E ist dahingehend sehr weit und bedarf dringend einer Konkretisierung. In der jetzigen Fassung dürfte die Thüringer Polizei sämtliche personenbezogene Daten aus dem Internet auslesen. Die Leitlinie der Kommission zu verbotenen Praktiken der künstlichen Intelligenz gemäß der Verordnung (EU) 2024/1689 (KI-Verordnung) sieht darin ein ungezieltes Auslesen. (siehe dazu Punkt 6.2.2. Durch ungezieltes Auslesen von Gesichtsbildern, Rn 228: „[...] kein besonderer Schwerpunkt auf bestimmte Einzelpersonen oder eine bestimmte Gruppe von Einzelpersonen gelegt wird.“). Sofern hier der Thüringer Polizei eine ungezielte Suche ermöglicht wird, sieht der TLfDI einen Verstoß gegen Art. 5 Abs. 1 lit. e) KI-VO.

Hingewiesen wird ferner auch auf das Urteil des Europäischen Gerichtshofs (EuGH) vom 19. März 2026 in der Rechtssache C-371/2 [Comdribus] (siehe dazu Pressemitteilung unter

<https://curia.europa.eu/site/upload/docs/application/pdf/2026-03/cp260039de.pdf>).

Dieses Urteil beschäftigte sich zwar inhaltlich mit erkennungsdienstlichen Maßnahmen in Form der Erhebung biometrischer Daten. Aber auch hier stellte der EuGH klar, dass erkennungsdienstliche Maßnahmen nicht systematisch angeordnet werden dürfen sondern klar begründet sein müssen.

Fraglich ist auch, welche Art von Daten zu Gesichtern zugrunde gelegt werden können (vollständige Daten zu Gesichtern, Ausschnitte von Gesichtern, bearbeitete Bilder, gezeichnete Bilder etc., siehe dazu auch Dr. Stephan Schindler, a.a.O., S. 6 f. mit Beispielen). Gleiches gilt für die in der Norm genannten „Stimmen“. Hierzu werden im vorliegenden Gesetzentwurf keine Aussagen getroffen. In der Gesetzesbegründung (S. 53) werden zudem auch Videos erwähnt. Der Umfang der einbezogenen Daten ist somit sehr weit.

Nach dem Wortlaut der Norm kann wohl der gesamte Polizeibestand in den Abgleich einbezogen werden. Auch die Gesetzesbegründung (S. 54) führt dahingehend aus, „[...] in den polizeilichen Informationssystemen gespeicherten Daten [...]“. Hier bedarf es einer Eingrenzung.

In dem Normtext selbst wird nicht festgelegt, ob die Polizei auch soziale Netzwerke durchforsten darf, die jedoch tatsächlich erst zugänglich sind, wenn man sich bei diesen registriert. Lediglich die Begründung zum Gesetzentwurf (S. 53) führt dazu aus, dass unter öffentlich frei zugänglichen Daten alle Daten zu verstehen sind, „die für jedermann ohne spezielle Registrierung sichtbar sind. Dies gelte auch für Bilder und Videos, beispielsweise aus sozialen Medien, soweit sich diese nicht an einen speziellen abgegrenzten Personenkreis richten.“ Eine gesetzliche Klarstellung sollte insofern vorgenommen werden.

Eine Eingrenzung der durchsuchbaren Internetbereiche, je nachdem, ob Informationen vorliegen, dass sich die Person nur in einem bestimmten bzw. bestimmbaren Bereich (z.B. die Person ist nur in einem bestimmbaren Medium vertreten) bewegt (siehe hierzu Dr. Stephan Schindler, a.a.O., S. 8), wurde normseitig nicht vorgenommen.

Hingewiesen wird ferner darauf, dass die Vorschrift den Zeitraum, der einem Abgleich zugrunde gelegt wird, nicht festlegt. Mangels Beschränkung des Zeitraums bestünde das Risiko, dass ein komplexes Bewegungsmuster erstellt oder Verhaltensanalysen einzelner Personen angelegt werden könnten.

Für den TLfDI stellt sich weiter die Frage, inwieweit der vom BVerfG definierte Schutz des Kernbereichs privater Lebensgestaltung hier konkret beachtet und eingehalten wird. Mit § 43a Abs. 3 PAG-E soll zwar der Kernbereichsschutz abgebildet werden. Die Formulierung „soweit möglich“ lässt Eingriffe in diesen aber zu. Hier bedarf es Nachbesserungen.

Die Norm sieht keine manuelle Überprüfungspflicht nach einem Abgleich vor.

§ 43a Abs. 5 PAG-E sieht eine Protokollierungspflicht vor. Weitere Kontrollmechanismen sind nicht vorgesehen. Ob dies für eine solche komplexe eingriffsintensive Maßnahme ausreichend ist, bleibt fraglich.

Bei einer Einführung einer so weitreichenden und eingriffsintensiven Maßnahme wie dem nachträglichen biometrischen Abgleich sollte mindestens die Aufnahme einer Evaluierungspflicht und ggfs. von Berichtspflichten an den Thüringer Landtag beinhaltet sein. Zudem ist zu überlegen, ob die Maßnahme einer zeitlichen Befristung bedarf (siehe dazu auch Dr. Stephan Schindler, a.a.O., S. 13, bzgl. einer zeitlich begrenzten Geltung sowie der Aufnahme von Berichts- und Evaluationspflichten).

Angesichts der Tragweite dieser sehr eingriffsintensiven Maßnahme, die eine unbestimmte Anzahl von Personen möglicherweise ungezielt erfasst und damit auch die Vereinbarkeit mit EU-Recht fraglich bleibt, spricht sich der TLfDI für eine Streichung der derzeitigen Fassung des § 43a PAG-E aus.

23. Zu Nr. 36 - § 45 PAG-E - Zuverlässigkeitsüberprüfung zum Schutz der Polizei:

Geprüft werden sollte, ob die Zuverlässigkeitsüberprüfung von Polizeibeamten im vorliegenden Thüringer Polizeigesetz geregelt werden kann bzw. soll. Die Aufnahme in ein beamtenrechtliches Verhältnis müsste grundsätzlich in den dafür vorgesehenen Gesetzen normiert werden. Diese Überlegungen gelten für Angestellte der Polizei entsprechend (siehe dazu auch: Der Hessische Beauftragte für Datenschutz und Informationsfreiheit, 51. Tätigkeitsbericht zum Datenschutz/ 5. Tätigkeitsbericht zur Informationsfreiheit, S. 72). Damit einhergehend ist auch die Frage, ob diese Datenverarbeitung unter die DS-GVO fällt oder unter den JI-Richtlinienbereich. Die Zuverlässigkeitsüberprüfung dient zudem grundsätzlich nicht der polizeilichen Gefahrenabwehr.

Fraglich ist, ob alle in § 45 Abs. 1 Nr. 1 - 4 PAG-E aufgeführten Personen einer so umfassenden Zuverlässigkeitsüberprüfung unterzogen werden sollten. Für nicht jeden Dienstleister und deren Mitarbeiter dürfte eine umfassende Überprüfung erforderlich sein. Dies sollte im Gesetz noch klarer herausgestellt werden. Mit dem

derzeitigen Wortlaut besteht die Gefahr, dass vorsorglich alle in den § 45 Abs. 1 Nr. 1 - 4 PAG-E aufgezählten Personengruppen einer Überprüfung unterzogen werden, um die Verantwortung einer Nicht-Überprüfung zu vermeiden.

Konkreter sollte § 45 Abs. 1 Nr. 1 PAG-E („Tätigkeit als Bedienstete bei der Polizei anstreben“) gefasst werden. Zu unbestimmt ist der dabei verwendete Begriff „anstreben“. Damit kann die Überprüfung weit vorgelagert werden, zu einem Zeitpunkt, in dem noch nicht klar ist, ob die Person tatsächlich bei der Polizei eingestellt werden möchte.

Konkreter sollte zudem geregelt werden, wer die Zuverlässigkeitsüberprüfung vornehmen darf. Im Gesetz wird ganz allgemein von „der Polizei“ gesprochen. Es empfiehlt sich, verfahrens- und organisationsrechtlich genau festzulegen, wer innerhalb der Polizei diese Überprüfung durchführen darf.

Bei § 45 Abs. 2 PAG-E ist zu prüfen, ob in die Vorschrift aufgenommen werden sollte, dass der Person, nachdem sie die Informationen erhalten hat, die Möglichkeit eingeräumt wird, von der Zuverlässigkeitsüberprüfung Abstand zu nehmen. So obliegt es ihrer Entscheidung, ob sie sich dem weiteren Verfahren stellen möchte oder auf die Tätigkeit bei oder im Zusammenhang mit der Polizei verzichtet.

Die in § 45 Abs. 3 PAG-E aufgezählten Datenbestände sollten konkretisiert werden. In der jetzigen Fassung ist eine umfassende Überprüfung mit sämtlichen Datenbeständen möglich. Es stellt sich die Frage nach der Verhältnismäßigkeit. Im Zusammenspiel mit § 45 Abs. 4 PAG-E findet eine umfassende Prüfung einer Person statt. Ob eine derartige Prüfung für jede in § 45 Abs. 1 Nr. 2 - 4 PAG-E aufgezählte Tätigkeit erforderlich ist, mag zu bezweifeln sein.

Aus der Sicht des TLfDI fehlen noch Ausführungen für den Fall, dass nach der erfolgten Zuverlässigkeitsüberprüfung eine Ablehnung der Person erfolgt. Allein die Möglichkeit, dass sich die Person an den Landesbeauftragten für den Datenschutz und die Informationsfreiheit wenden kann (§ 45 Abs. 2 Nr. 4 PAG-E), dürfte

für einen effektiven Rechtsschutz nicht abschließend sein. Aufgenommen werden sollte auch die Möglichkeit für die betroffene Person, dass ihr zu den vorliegenden Erkenntnissen aus der Zuverlässigkeitsüberprüfung die Möglichkeit zur Stellungnahme gegeben wird. Hinzuweisen ist an dieser Stelle, dass bei einer Auskunftserteilung nach dem Thüringer Verfassungsschutzgesetz die Ablehnung keiner Begründung bedarf, soweit dadurch der Zweck der Auskunftsverweigerung gefährdet würde (§ 17 Abs. 4 ThürVerfSchG). So kann es passieren, dass die betroffene Person gegebenenfalls abgelehnt wird aufgrund von Erkenntnissen des Thüringer Verfassungsschutzes, sie aber nie erfahren würde, um welche Erkenntnisse es sich dabei handelt. (siehe hierzu auch: Der Hessische Beauftragte für Datenschutz und Informationsfreiheit, a.a.O., S. 72). Ferner wird an dieser Stelle auf das Trennungsgebot zwischen der Polizei und dem Verfassungsschutz hingewiesen.

In § 45 Abs. 4 PAG-E werden die Kriterien vorgegeben, an denen sich die Polizei bei der Entscheidung über die Zuverlässigkeit einer betroffenen Person orientieren kann. Die Kriterien sind teilweise sehr weit gefasst. Zu prüfen ist, ob hier eine Begrenzung vorzunehmen ist. In der jetzigen Fassung wird die betroffene Person einer sehr umfassenden Betrachtung unterzogen. Eine Abstufung nach der Tätigkeit der betroffenen Person erfolgt gesetzlich nicht.

Gem. § 45 Abs. 4 UAbs. 2 Nr. 1 PAG-E kommen als sonstige Erkenntnisse insbesondere laufende oder eingestellte Ermittlungs- oder Strafverfahren in Betracht. Insbesondere bei laufenden Verfahren ist fraglich, welche Erkenntnisse daraus gewonnen werden können, weil in diesem Verfahrensstadium gerade noch keine Entscheidung vorliegt.

Bedenklich sind die in § 45 Abs. 4 UAbs. 2 Nr. 3 PAG-E genannten Kriterien, die Zweifel an der Zuverlässigkeit einer betroffenen Person ergeben sollen. Dies betrifft die Alkohol-, Rauschmittel- oder Medikamentenabhängigkeit oder den regelmäßigen Missbrauch dieser Substanzen. Dies geht weit in die Privatsphäre der betroffenen Person und sollte aus datenschutzrechtlicher Sicht gestrichen werden. Fraglich ist zudem, wie die Polizei diese Daten erhebt. Es handelt sich dabei unter Umständen auch um Gesundheitsdaten, die zu den sensibelsten Datenkategorien

zählen. Zu Bedenken ist ferner, dass es sich unter Umständen auch nur um Verdachtsmomente handeln kann. Wird eine Person auf dieser Grundlage abgelehnt, kann das ggfs. sehr weitreichende berufliche Konsequenzen nach sich ziehen. Hinzu kommt, dass die Person nach dem derzeitigen Wortlaut der Norm nicht die Möglichkeit hat sich zu etwaigen Verdachtsmomenten, die gegen sie vorliegen, zu äußern bzw. falsche Daten zu korrigieren.

Keine Angaben macht das Gesetz, welche Zeiträume in § 45 Abs. 4 PAG-E zugrunde gelegt werden. Im Moment gibt es keine Einschränkungen, sodass grundsätzlich auf jegliche Ereignisse, die zu dieser Person vorliegen, zurückgegriffen werden darf. Zu prüfen ist, inwiefern hier eine Einschränkung erfolgen muss.

Nach § 45 Abs. 5 PAG-E sind Wiederholungsprüfungen zulässig, wenn seit der letzten Überprüfung mindestens ein Jahr vergangen ist. Aufgenommen werden sollte eine Dokumentationspflicht zu den Gründen, die eine Wiederholungsprüfung rechtfertigen. Hingewiesen wird an dieser Stelle, dass durch die Wiederholungsprüfungen die Gefahr besteht, dass die betroffenen Personen einer dauerhaften Kontrolle unterliegen. Fraglich ist, ob dies verhältnismäßig ist.

Die Speicherung der Verfahrensunterlagen ist in § 45 Abs. 6 PAG-E normiert. Es fehlt eine Regelung, dass Erkenntnisse, die nicht in die Prüfung eingeflossen sind, zu löschen sind. Konkretisiert werden sollte der Begriff „Rechtsstreit“. Von hiesiger Seite ist nicht klar erkennbar, ob damit nur der Rechtsstreit bezüglich der Zuverlässigkeitsüberprüfung gemeint ist oder es sich auf sämtliche Rechtsstreitigkeiten bezieht. Unklar bleibt auch die Formulierung „voraussichtlich zu erwartenden Rechtsstreit“, da ein solcher in jedem Fall möglich sein kann und somit die Gefahr besteht, dass die Daten aus diesem Grund weiter vorgehalten werden. Laut der Vorschrift kann die betroffene Person aus einem anderen Anlass erneut einer Zuverlässigkeitsüberprüfung unterzogen werden. Nicht bestimmt ist, was unter „einem anderen Anlass“ zu verstehen ist.

Hingewiesen wird darauf, dass in der Begründung (S. 56) von „Antragsunterlagen mit der schriftlichen Einwilligung“ gesprochen wird. Fraglich ist, welche Einwilligung hier gemeint ist.

Aufgenommen werden müsste schließlich die Klarstellung, dass die Datenverarbeitung aus einer Zuverlässigkeitsüberprüfung getrennt von dem polizeilichen Datenbestand erfolgt. Darüber hinaus ist gesetzlich zu normieren, dass diese Daten nicht einer Datenanalyse (§ 40a PAG-E) zugeführt werden, gerade weil sie eigentlich nicht für Gefahrenabwehrzwecke bestimmt sind bzw. diese nur sehr entfernt berühren. Die betroffene Person wird hier lediglich wegen ihres Berufs oder ihrer auszuübenden Tätigkeit bei der Polizei bzw. im Zusammenhang mit der Thüringer Polizei überprüft.

Im Zusammenhang mit der Zuverlässigkeitsüberprüfung regt der TLfDI an, die Zuverlässigkeitsüberprüfung für Anlässe, die mit erheblichen Sicherheitsrisiken verbunden sind (z.B. Fußballweltmeisterschaft) in einer gesetzlichen Vorschrift zu regeln. Beispielhaft für eine solche Norm ist § 60a Polizeiaufgabengesetz Bayern, an der sich dabei orientiert werden kann.

III. Anmerkungen zu dem übersandten Fragenkatalog

Zu dem übersandten Katalog, der insgesamt 141 Fragen beinhaltet, ist es aufgrund der angespannten Personalsituation beim TLfDI leider nicht möglich, auf alle Fragen einzugehen. Eine Äußerung erfolgt deshalb nur zu ausgewählten Fragestellungen. Die wesentlichen Kritikpunkte entnehmen Sie bitte der Stellungnahme. Soweit möglich, hat sich der TLfDI darin bereits auf die konkreten Fragen bezogen.

A) Grundsätzliche Fragen

Frage 2:

Mehrere der zentralen neuen Befugnisse des Entwurfs erlauben tiefgreifende Eingriffe bereits im Vorfeld konkreter Straftaten. Wie bewerten Sie aus Ihrer Sicht diese Verschiebung des Polizeirechts vom klassischen Gefahrenabwehrrecht hin zu einem präventiven Sicherheitsrecht, das teilweise auf bloße Prognosen künftigen

Verhaltens abstellt? Sehen Sie hier noch tragfähige Grenzen zum Bestimmtheitsgebot des Art. 20 Abs. 3 Grundgesetz (GG) oder besteht die Gefahr, dass sich das Polizeirecht strukturell vom Prinzip der „Gefahr“ entfernt und zu einem präventiven Kontrollrecht entwickelt?

Antwort:

Ob sich das Polizeirecht strukturell vom Prinzip der „Gefahr“ entfernt und sich zu einem präventiven Kontrollrecht entwickelt, hat der Thüringer Gesetzgeber selbst in der Hand. Jeder Grundrechtseingriff bedarf einer verfassungsgemäßen Rechtfertigung. Je schwerer der Eingriff in die Grundrechte der Menschen ist, desto höher sind unter anderem die Anforderung an die Bestimmtheit einer Norm sowie hinreichende Eingriffsschwellen, eine konkrete und strikte Zweckbindung, der Umfang der Daten, die Qualität der Daten, angemessene Löschfristen, effektive Rechtsschutzmöglichkeiten und unabhängige Kontrollmechanismen.

Frage 3:

Wenn man die im Entwurf vorgelegten Instrumente im Zusammenspiel betrachtet: Sehen Sie hier die Entstehung einer neuen Form datengetriebener Polizeiarbeit, bei der große Mengen Daten unbeteiligter Personen systematisch erfasst und analysiert werden können - auch vor dem Hintergrund einer gegebenenfalls künftigen autoritären Regierung in Thüringen - oder halten Sie dieses Risiko für völlig unbegründet?

Antwort:

Einige Maßnahmen können bei einer Einzelbetrachtung durchaus sinnvoll sein. Im Zusammenspiel besteht aber die Gefahr, dass damit umfangreiche Analysen ermöglicht werden könnten. Andere Maßnahmen bergen bereits jetzt das Risiko, dass hier eine Vielzahl unbeteiligter Personen betroffen sind, wie z.B. bei § 43a PAG-E. Aus diesem Grund ist es wichtig, dass der Gesetzgeber gerade bei solchen eingriffsintensiven Maßnahmen hinrei-

chend bestimmte Normen erlässt. Gleichzeitig müssen die einzelnen Maßnahmen auch im Zusammenhang mit ihrer zweckändernden Weiterverarbeitung betrachtet werden. Diese muss auf das erforderliche Maß begrenzt werden. Es sollte geprüft werden, ob die Gesamtheit der polizeilichen Maßnahmen im Gesetz dazu führt, dass eine Person oder Personen einer potenziellen dauerhaften polizeilichen Beobachtung unterworfen werden könnten.

Frage 4:

Wo liegen aus datenschutz- und grundrechtlicher Sicht die Grenzen einer solchen datengetriebenen Polizeiarbeit und erfüllt der vorliegende Entwurf diese Anforderungen nach Ihrer Einschätzung?

Antwort:

Im PAG-E sind in der derzeitigen Fassung neue Befugnisse vorgesehen, wie z.B. die elektronische Aufenthaltsüberwachung, ein nachträglicher biometrischer Abgleich mit öffentlich frei zugänglichen personenbezogenen Daten aus dem Internet, eine automatisierte Datenanalyse und neue technische Verfahren zur Verhaltensmustererkennung.

Für diese Befugnisse bedarf es, wie bereits oben erwähnt, formell und materiell rechtmäßiger Rechtsgrundlagen, die nicht gegen höherrangiges Recht verstoßen. Im Rahmen der Stellungnahme wurden seitens des TLfDI bei den einzelnen Normen Probleme angesprochen (siehe z.B. die Ausführungen zu § 43a PAG-E) auf die an dieser Stelle verwiesen wird.

Um einer vermeintlichen datengetriebenen Polizeiarbeit Grenzen aufzusetzen, bedarf es grundsätzlich auch einer möglichst hinreichenden Transparenz der Maßnahmen, eines effektiven Rechtsschutzes betroffener Personen sowie einer Nachvollziehbarkeit polizeilichen Handelns (z.B. Protokollierungspflichten, oder ob z.B. KI eingesetzt wird).

Frage 6:

Reichen die vorgesehenen Kontrollmechanismen aus, um die erheblichen Grundrechtseingriffe effektiv zu begrenzen, oder sehen Sie strukturelle Defizite bei Richtervorbehalten, Transparenz und unabhängiger Kontrolle? Fehlen aus Ihrer Sicht Änderungen im PAG, die gar nicht Bestandteil des vorgelegten Entwurfs sind? Wenn ja, welche schlagen Sie vor?

Antwort:

Dem TLfDI ist bekannt, dass auch die Polizei in Thüringen an P20 teilnehmen möchte. Es wird darauf hingewiesen, dass im PAG-E die entsprechenden Regelungen dafür ergänzt oder überarbeitet werden müssen. Insbesondere wird dazu das Rechtsgutachten von Prof. Dr. Matthias Bäcker, LL.M., Universität Mainz empfohlen, das im Auftrag des damaligen Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum polizeirechtlichen und verfassungsrechtlichen Rahmen eines polizeilichen Informationsverbunds der Länder erstellt wurde. Abrufbar ist das Gutachten unter:

<https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Dokumente-allg/2023/Gutachten-polizeilicher-Informationsverbund.html>

In diesem Gutachten wird auf Seite 3 unter 5. auf Nachschärfungen in den Polizeigesetzen der beteiligten Länder verwiesen. Dies sollte auch Thüringen zum Anlass nehmen und prüfen, ob die gesetzlichen Grundlagen für P20 vorhanden sind und ggfs. einer Anpassung bedürfen.

Der TLfDI spricht sich erneut dafür aus, die sogenannte „Mitziehklausel“ zu streichen. Diese besagt, dass, soweit innerhalb der Speicherfrist für ein Ereignis – aufgrund eines neuen Ereignisses – eine weitere Speicherung hinzukommt, das für den neuen Fall berechnete Prüfdatum bzw. die Prüffrist (aus § 40 Abs. 6 ThürPAG in Verbindung mit ThürPolPrüffristVO) für die gesamte Speicherung maßgeblich wird; es kommt damit zum einem „Neustart“ der jeweiligen Prüffrist. Aufgrund der neuen Speicherung unterfallen

weiter zurückliegende Ereignisse letztendlich der festgesetzten neuen Prüffrist. Vor dem Hintergrund, dass der PAG-E neue polizeiliche Maßnahmen vorsieht und damit einhergehend die Datenmenge quantitativ weiter steigen wird, wäre dies auch ein probates Mittel, den polizeilichen Datenbestand auf ein grundrechtsschonendes Mindestmaß zu reduzieren.

Gleichzeitig wird ganz grundsätzlich empfohlen, die Fristen der polizeilichen Datenspeicherung einer genauen Überprüfung unterziehen und ggfs. zu kürzen.

Frage 9:

Haben Sie datenschutzrechtlichen Bedenken bei Einzelregelungen des Gesetzesentwurfes? Gibt es bestimmte zusätzliche Sicherungsmaßnahmen, die Sie anregen würden?

Antwort:

Siehe hierzu die Ausführungen in der Stellungnahme.

Frage 15:

Der Schutz des Kernbereichs privater Lebensgestaltung stellt nach der Rechtsprechung des Bundesverfassungsgerichts eine zentrale Grenze staatlicher Überwachung dar. Halten Sie die im Gesetzesentwurf vorgesehenen Schutzmechanismen und Verfahrensvorkehrungen für ausreichend, um diesen Bereich effektiv zu schützen?

Antwort:

Der Kernbereich der privaten Lebensgestaltung ist absolut geschützt und darf nicht gezielt ausgeforscht werden.

Nach § 43a Abs. 3 PAG-E ist jedoch „[...] soweit möglich, technisch sicherzustellen, dass Daten die den Kernbereich der privaten Lebensgestaltung betreffen, nicht erhoben werden [...]“. Durch die Formulierung „soweit mög-

lich“ werden Eingriffe zugelassen. Der Schutz der privaten Lebensgestaltung kann dann unter Umständen erst nach der Erhebung greifen. Das müsste geändert werden.

Hingewiesen wird darauf, dass auch bei der Videoüberwachung mit Mustererkennung und Nachverfolgungsfunktion nach § 33 PAG-E und der elektronischen Aufenthaltsüberwachung nach § 34g PAG-E mögliche andere sensible Bereiche betroffen sein können, auch wenn unter Umständen nicht den Kernbereich der privaten Lebensgestaltung berührt wird.

Frage 16:

Der Gesetzentwurf nimmt Bezug auf moderne Methoden der Bilderkennung. Welche verfassungsrechtlichen und datenschutzrechtlichen Risiken sehen Sie beim Einsatz solcher Technologien im öffentlichen Raum, insbesondere im Hinblick auf eine mögliche flächendeckende Identifizierbarkeit von Personen?

Antwort:

Siehe hierzu die Ausführungen in der Stellungnahme bei den jeweiligen Maßnahmen.

Frage 17:

Welche Auswirkungen könnten aus Ihrer Sicht weitreichende Befugnisse zur Datenauswertung und technischen Überwachung auf das Vertrauen der Bevölkerung in den Staat und seine Sicherheitsbehörden haben?

Antwort:

Starke Befugnisse der Polizei könnten zu einem vermeintlich erhöhten Sicherheitsempfinden in der Bevölkerung führen. Der vorliegende Entwurf kann aber auch dazu führen, dass durch das Zusammenspiel der einzelnen Maßnahmen der Eindruck, aber auch die reale Gefahr entstehen kann, dass die Menschen vorsorglich einer polizeilichen Beobachtung unterwor-

fen werden, diese Daten dann analysiert und ausgewertet bzw. bewertet werden. Dabei wird auch eine nicht unerhebliche Anzahl von Personen erfasst, die durch ihr Alltagsverhalten überhaupt keinen Anlass für etwaige polizeiliche Maßnahmen geben. Dies betrifft beispielsweise die polizeiliche Videoüberwachung (ggfs. mit Hilfe von Drohnen) und den nachträglichen biometrische Abgleich mit öffentlich frei zugänglichen personenbezogenen Daten.

Die Polizeiarbeit darf insofern nicht ausufern, die Eingriffe müssen auf einer formell und materiell rechtmäßigen Rechtsgrundlage basieren, nachvollziehbar und kontrollierbar sein.

B) Fachfragen zu einzelnen Normen

Zu § 14

Frage 21:

Im Entwurf werden lediglich die Worte „der unerlaubten Überschreitung der Landesgrenze oder“ in § 14 Abs. 1 Nr. 5 gestrichen, ist damit dem Änderungsbedarf in §14 Genüge getan oder braucht es aus ihrer Sicht weitergehende Änderungen in § 14 Abs. 1 Nr. 2 a) aa) vor dem Hintergrund der Unbestimmtheit so genannter „Gefahrengebiete“ / „gefährlicher Orte“ in Thüringen, die ihrer Konstruktion neben anlasslosen Personalienfeststellungen (§ 14) etwa auch Durchsuchungen von Personen (in § 23) erlauben und in der Vergangenheit- abseits formalisierter Festlegungen lediglich in einer von sieben Landespolizeiinspektionen, der LPI Erfurt - in verschiedenen Städten ohne Dokumentation und Anordnung durch die Behördenleitung sondern durch vor Ort handelnden Polizeibeamtinnen und -beamten teils stündlich ad hoc erklärt wurden, um anlasslose Kontrollen ohne konkreten Straftat oder Gefahrenverdacht zu begründen, was wiederholt in parlamentarischen Vorgänge mündete? [vgl. beispielhaft Antworten des Innenministeriums auf Parlamentsanfragen Drucksache 7/8762, 7/8780 u.a. und Schreiben der LPI Jena bei FragDenStaat.de, etwa vom 25. Mai 2025]

Antwort:

§ 14 PAG-E sieht in der jetzigen Entwurfsfassung lediglich die Streichung der Worte „der unerlaubten Überschreitung der Landesgrenze oder“ vor.

Nach § 14 Nr. 2 Abs. 1 Buchst. a) aa) kann die Polizei die Identität einer Person feststellen, „wenn die Person sich an einem Ort aufhält, von dem aufgrund tatsächlicher Anhaltpunkte anzunehmen ist, dass dort Personen Straftaten verabreden, vorbereiten oder verüben.“

Sofern in der Vergangenheit Schwierigkeiten bestanden, unter welchen Voraussetzungen ein gefährlicher Ort angenommen werden darf, empfiehlt sich eine gesetzliche Konkretisierung, damit die Norm dem Bestimmtheitsgrundsatz genügt.

In diesem Zusammenhang wird darauf hingewiesen, dass gem. § 33 Abs. 2 Nr. 1 PAG an einem „öffentlich zugänglichen Ort, soweit tatsächliche Anhaltpunkte die Annahme rechtfertigen, dass dort Straftaten verabredet, vorbereitet oder verübt werden sollen“, eine Videoüberwachung des öffentlichen Raums zulässig sein kann. Gemeint sind dabei etwaige Kriminalitätsschwerpunkte. Die Videoüberwachung stellt einen nicht unerheblichen Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar. Aufgrund der Streubreite wird auch eine Vielzahl von Personen erfasst, die gerade nicht wegen ihres Verhaltens einen Anlass für die Maßnahme gegeben haben. Hinzu kommen nach dem Gesetzentwurf die Verhaltensmustererkennung und eine Nachverfolgungsfunktion. Aus diesem Grund wird empfohlen, die Eingriffsschwelle in § 33 Abs. 2 Nr. 1 PAG anzuheben. Als Beispiel könnte hier § 57 Abs. 3 Nr. 2 SächsPVDG dienen.

Zu § 18a

Frage 27:

Wie bewerten Sie die vorgesehenen Datentransfers an Beratungsstellen und Interventionsstellen? Sind Zweckbindung, Freiwilligkeit, Löschlogik und informatio-

nelle Selbstbestimmung ausreichend abgesichert, oder drohen aus Ihrer Sicht Risiken durch die vorgesehene Änderung?

Antwort:

Siehe hier die Ausführungen in der Stellungnahme.

Zu § 21

Frage 29:

Wie bewerten Sie die verfassungsrechtliche Angemessenheit, im Freiheitsentzug

a) eine Videoüberwachung und

b) eine automatisierte Mustererkennung „Verhaltensmuster“

zuzulassen? Ist das aus Ihrer Sicht ein unverhältnismäßiger Intensivierungsschritt, weil Gewahrsamspersonen besonders vulnerabel sind, oder dient diese Regelung überwiegend dem Schutz der in Gewahrsam genommenen Person, auch mit Blick auf Suizidprävention und Schutz vor unverhältnismäßigen polizeilichen Zwangsanwendungen?

Antwort:

Siehe hier die Ausführungen in der Stellungnahme.

Frage 32:

Welche gesetzlichen Änderungen empfehlen Sie, damit Gewahrsamsüberwachung nicht zur Normalität wird? Sollte aus Ihrer Sicht - ähnlich wie im bereits geltenden § 33a PAG (Bodycam) - auch das polizeiliche Gegenüber die Möglichkeit erhalten, eine Aufzeichnung der Gewahrsamsräume zu verlangen?

Antwort:

Wie bereits in der Stellungnahme ausgeführt, wäre zu prüfen, ob es nicht grundrechtsschonender ist, auf eine Videoaufzeichnung komplett zu ver-

zichten und stattdessen die reine Beobachtung eines Gewahrsamsraumes ausreichen zu lassen.

Zu § 30

Frage 39:

Wie bewerten Sie § 30a in seiner Abgrenzung zu Zeugenschutz und Sicherheitsinstrumenten, insbesondere zum Gesetz zur Harmonisierung des Schutzes gefährdeter Zeugen (ZSHG)? Ist die polizeirechtliche Verankerung verfassungs- und datenschutzrechtlich unproblematisch, oder entsteht eine Parallelstruktur mit unklaren Zuständigkeiten und Kontrolllücken?

Antwort:

Um Unklarheiten zu vermeiden, sollte ggfs. aufgenommen werden, in welchem Verhältnis § 30a PAG-E zu dem ZSHG steht und wie eine Koordinierung mit den Strafverfolgungsbehörden und Zeugenschutzdienststellen (§ 2 ZSHG) erfolgt. Kontrolllücken könnten durch eine unabhängige Kontrollstelle geschlossen werden.

Die in § 6 ZSHG aufgeführten Regelungen sollten auch in § 30a PAG-E aufgenommen werden.

Zu § 33

Frage 46:

Wie bewerten Sie die vorgesehenen Regelungen zum KI-Einsatz sowie die Darstellung in der Begründung des Gesetzentwurfs, dass es sich um ein bereits austrainiertes System handelt, auch mit Blick auf Risiken durch Bias und Diskriminierung? Ist Ihnen bekannt, ob diese Produkte fehlerfrei agieren oder in welcher Weise es zu falschpositiven oder falsch-negativen Meldungen kommt?

Antwort:

Es soll sich um ein austrainiertes System handeln, welches sich während der Erkennung und Auswertung der Muster weder weiterentwickelt noch dazulernt (vor allem nicht mit polizeilichen Daten). Leider wird dies nur in der Gesetzesbegründung erwähnt (S. 37). Eine Normierung im Gesetz hätte dahingehend mehr Klarheit.

Hinzuweisen ist an dieser Stelle, dass auch austrainierte KI-Systeme immer eine Fehlerrate aufweisen. Dies hängt z.B. von der Beleuchtung, den Wetterverhältnissen, der Verschmutzung oder der Kennzeichenverformung, -verdeckung ab. Auch ein Bias ist systemimmanent, wobei ausgereifte Kennzeichenerkennungssysteme hier genügend große Trainingsdaten zur Verfügung hatten, um kaum noch Bias aufzuweisen. Hier dürften Bias-Effekte im entfernten Nicht-Europäischen Raum auftreten. Unbekannt ist der Bias in Aktivitätserkennungssystemen (in welchen Schlägereien, Messerangriffe, Raubüberfälle erkannt werden sollen). Aufgrund des beschränkten Trainingsmaterials ist zu vermuten, dass dort auch ein ethnischer Bias vorhanden sein könnte oder ein Bias bezüglich des Geschlechts. Beide Bias-Quellen sind nur implizit im System hineintrainiert, aber wahrscheinlich nachweisbar. Unklar ist jedoch, ob der vorhandene Bias Auswirkungen auf die Tauglichkeit des Systems hat. Dazu liegen dem TLfDI keine Informationen vor.

Frage 48:

Im Mai 2025 warnten das BSI und internationale Sicherheitsdienste vor massiven Hackerangriffen auf Kamera-Systeme in Europa, auch im öffentlichen Raum, verübt durch eine Einheit des russische Militärgesheimdienstes APT28. 2026 wurde zudem nach einem Bericht der Financial Times ein mehrjähriger umfassender Zugriff eines ausländischen Geheimdienstes auf das Netz von tausenden Verkehrskameras in einer Großstadt im Nahen Osten bekannt. Halten Sie angesichts der Bedrohungslage in Europa und weltweit einen weiteren Ausbau von Videoüberwachung im öffentlichen Raum in Thüringen, teils auch mit KI wie in § 33 vorgesehen

dahingehend für riskant, dass die Technik sich als digitaler Bumerang erweisen könnte, bei der auch KRITIS-Einrichtungen in Thüringen und Bedienstete der Thüringer Polizei, andere Sicherheitsbehörden oder Mitglieder der Landesregierung durch Kriminelle und Nachrichtendienste anderer Länder über Sicherheitslücken in dieser geschaffenen Struktur ausgespäht werden könnten?

Antwort:

Es ist nicht neu, dass Kriminelle und Nachrichtendienste anderer Länder über Sicherheitslücken oder gezielte Angriffe geschaffene Strukturen ausspähen und ausgespäht haben.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist die Cybersicherheitsbehörde des Bundes. Sie beobachtet kontinuierlich die Lage der IT-Sicherheit in Deutschland. Sie stellte auch in ihrem letzten Jahresbericht fest, dass generell die IT-Sicherheitslage in Deutschland weiterhin auf einem angespannten Niveau bleibt

(<https://medien.bsi.bund.de/lagebericht/de/zusammenfassung-und-bewertung/>). Das BSI warnt zudem regelmäßig Bürger und Hersteller vor Sicherheitslücken (§ 13 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen (BSI-Gesetz - BSIG),

https://www.gesetze-im-internet.de/bsig_2025/BSIG.pdf), so auch zu Videoüberwachungssystemen, da diese auch als Einfallstor für Hacker dienen können. Zudem aktualisiert das BSI regelmäßig seine Hinweise zu Videoüberwachungssystemen:

<https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Internet-der-Dinge-Smart-leben/Smart-Home/Smarte-Ueberwachungskameras/smart-ueberwachungskameras.html>.

Was die KRITIS-Einrichtungen betrifft, so sind analog § 30 BSIG entsprechende Risikomanagementmaßnahmen dem Stand der Technik zu ergreifen.

Frage 49:

Wie hoch ist die zu erwartende Falsch-Positiv-Rate bei der automatisierten Verhaltenserkennung aus Videoüberwachung und wie bewerten Sie die damit verbundenen Grundrechtseingriffe bei unbeteiligten Personen?

Antwort:

In gutartigen Fällen können 1% bis 10% Falsch-Positiv-Rate erzielt werden. Die Raten können aber auch auf über 50% steigen, was einfachem Raten gleichkommt (siehe <https://link.springer.com/content/pdf/10.1007/s10462-025-11206-w.pdf>). Es ist somit insbesondere in der Anfangszeit von zahlreichen Fehlalarmen auszugehen.

Zu § 33c

Frage 55:

Welches Risiko entsteht aus der vorgesehenen Bewegungsmusterverfolgung?

Antwort:

Gem. § 33c Abs. 3 PAG-E ist eine Verwendung der Daten zur Erstellung eines Bewegungsprofils mit Ausnahme der Fälle des § 14 Abs. 1 Nr. 6 unzulässig. In diesem Fall besteht die Möglichkeit, ein Bewegungsprofil zu erstellen. Zu prüfen ist, ob diese Möglichkeit konkreter ausgestaltet werden muss, z.B. mit einer genaueren Zweckfestlegung, einem genauen Zeitraum, wem die Kontrolle über die Maßnahme obliegt und ob ggfs. ein Richtervorbehalt vorliegen muss.

Zu § 34g

Frage 74:

Der Entwurf bündelt sehr unterschiedliche Anwendungsfälle (von KRITIS über „gewaltbereite Extremisten“ bis hin zu häuslicher Gewalt). Sehen Sie darin ein Ri-

siko der Zweckausweitung „Opferschutz als Türöffner“? Wenn ja, wären Limitierungen aus Ihrer Sicht erforderlich und welche?

Antwort:

Der Gesetzentwurf legt in § 34g Abs. 1 Nr. 1 - 4 PAG-E fest, in welchen Fällen eine elektronische Aufenthaltsüberwachung in Betracht kommt. Sofern einzelne Zwecke nicht vom Gesetzgeber gewollt sind, müsste dieser die dazu erforderlichen Anpassungen vornehmen und den Anwendungsbereich strenger limitieren. Eine elektronische Aufenthaltsüberwachung stellt eine Maßnahme dar, mit der besonders tief in Grundrechte der betroffenen Person eingegriffen wird. Daher ist es wichtig, die Anwendungsbereiche nicht ausufern zu lassen und auf den vom Gesetzgeber gewollten Zweck streng zu begrenzen. Zu beachten ist auch, dass nach dem derzeitigen Wortlaut des § 34g Abs. 3 PAG-E Zweckänderungen der erhobenen Daten zulässig wären. Die Datenverarbeitung wird dadurch noch weiter ausgeweitet.

Frage 76

Halten Sie es für verhältnismäßig, eine derart eingriffsintensive Maßnahme wie die elektronische Aufenthaltsüberwachung bereits zur Abwehr einer einfachen Gefahr für die „Gesundheit einer Person“ oder zur Abwehr einer Gefahr für „sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen“ zu ermöglichen, auch wenn keinerlei Bezug zu Partnerschaftsgewalt o.ä. vorliegt, sondern hier schlicht allgemein einfache Gefahren in den Blick genommen werden, die weder eine erhebliche noch eine dringende Gefahr für besonders gewichtige Rechtsgüter oder eine konkretisierte Gefahr schwerer Straftaten begründen?

Antwort:

Siehe hier die Ausführungen in der Stellungnahme.

Zu § 38

Frage 87:

Welche zusätzlichen Grundrechtsrisiken entstehen aus Ihrer Sicht, wenn Drohnen künftig regelhaft als Plattform für Datenerhebung im vorgesehenen Umfang genutzt werden, auch mit Blick auf die Rechte von Menschen, die sich bei Ansammlungen und Veranstaltungen aufhalten, sowie mit Blick auf die Abgrenzung zu Versammlungen?

Antwort:

Eine eigene Datenerhebungsbefugnis sieht § 38 PAG-E nicht vor.

Die Drohne kann im Rahmen von § 33 PAG, als besonders Mittel nach § 34 Abs. 2 Nr. 1 und 2 PAG oder bei § 34c PAG eingesetzt werden. Eine Drohne hat eine größere Reichweite und ist sehr flexibel. Damit ist es möglich Menschenmengen leichter zu überblicken, aber auch zu überwachen. Dies betrifft in der Regel auch eine Vielzahl von Personen, die anlasslos mitüberwacht werden. Gleichzeitig ist eine Drohne schwerer zu erkennen. In der Gesamtschau mit § 33 PAG können beispielsweise zukünftig bei öffentlichen Veranstaltungen und Ansammlungen mit einer Drohne Aufzeichnungen erfolgen, diese automatisch ausgewertet und zur Nachverfolgung von Personen genutzt werden. Dieses Szenario muss sich der Gesetzgeber bewusst sein. Andernfalls bedarf es einer weiteren Eingrenzung des Einsatzes von Drohnen.

Der Gesetzeswortlaut schreibt zudem vor, dass die Offenheit der Maßnahme gewahrt bleibt. Auf die Verwendung der Drohne soll nach dem Wortlaut gesondert hingewiesen werden. Von hiesiger Seite wird angemerkt, dass eine „Soll-Vorschrift“ gerade keine abschließende Verpflichtung ist.

Zu § 43a

Frage 106:

Gehen mit dem neuen § 43a aus Ihrer Sicht grund- und menschenrechtliche Risiken einher, mit Blick auf biometrische Massenbetroffenheit, Fehlzusammenhänge,

Diskriminierung und sogenannte Chilling Effects?

Antwort:

Siehe hierzu die Ausführungen in der Stellungnahme.

Frage 107:

Wie bewerten Sie die Schwelle „aussichtslos oder wesentlich erschwert“ als Begrenzung?

Antwort:

Die Schwelle „aussichtslos“ kann grundsätzlich vertretbar sein, weil vorher alle anderen Lösungswege erfolglos ausgeschöpft wurden. Anders ist die Schwelle „wesentlich erschwert“ zu beurteilen. Diese Schwelle ist deutlich schwächer und kann eine Vielzahl von Möglichkeiten einfließen lassen, nach deren Bewertung dann die Maßnahme nach § 43a PAG-E als „wesentlich erleichternde Maßnahme“ erfolgen könnte. Für das Vorliegen einer wesentlichen Erschwernis könnte seitens der Polizei unter Umständen leicht begründet werden, dass andere Maßnahmen zur Abwehr der Gefahr auf andere Weise z.B. (zeit)aufwendiger oder personaltechnisch schwieriger umzusetzen wären.

Frage 108:

Entspricht § 43a aus Ihrer Sicht den Anforderungen einer strengen Zweck- und Schwellenbindung im europäischen Datenschutzrahmen, oder fehlen zentrale Schutzvorkehrungen?

Antwort:

Die datenschutzrechtlichen Bedenken bezüglich der Norm entnehmen sie bitte den Ausführungen aus der Stellungnahme.

Frage 109:

Besteht aus Ihrer Sicht das Risiko, dass auf die Daten massenhaft drittbetroffener, unbescholtener Bürgerinnen und Bürger - etwa in sozialen Medien wie Instagram oder Facebook - zugegriffen wird beziehungsweise diese biometrisch ausgewertet werden? Wenn ja: Können Sie abschätzen, wie groß die Dimension dieser Drittbetroffenheit

Antwort:

Laut der Gesetzesbegründung (S. 53) sind frei zugängliche Daten aus dem Internet alle Daten zu verstehen, die für jedermann ohne spezielle Registrierung sichtbar sind. Dies gelte – nach der Begründung – auch für Bilder und Videos, beispielsweise aus sozialen Medien, soweit sich diese nicht an einen spezifisch abgegrenzten Personenkreis richten. Insofern ist eine Drittbetroffenheit einer nicht unerheblichen Anzahl von Personen sehr wahrscheinlich.

Frage 110:

Welche Rolle spielen aus Ihrer Sicht Fehlerraten und Bias der eingesetzten Systeme? Welche rechtlichen Sicherungen sind nötig, damit biometrische Treffer nie alleinige Entscheidungsgrundlage für Folgeeingriffe werden?

Antwort:

Bias spielt in der biometrischen Erkennung auch eine Rolle. Falsch-Identifikationen sind nicht auszuschließen. Nach Auffassung des TLfDI muss jede Identifikation durch eine Person geprüft werden.

Frage 111:

Sehen Sie mit der vorgeschlagenen Regelung Vollzugs- und Missbrauchsrisiken

entstehen, oder ist sie aus Ihrer Sicht auch vor dem Hintergrund von EU-Verordnungen und perspektivischen Anforderungen etwa aus der EU-KI-Verordnung geeignet ausgestaltet?

Antwort:

Siehe hierzu die Ausführungen in der Stellungnahme.

Frage 112:

Wie bewerten Sie den Richtervorbehalt in § 43a?

Antwort:

Der Richtervorbehalt ist angesichts der Eingriffsintensität der Maßnahme eine zu begrüßende Aufnahme in den Gesetzentwurf.

Frage 114:

Wie bewerten Sie das Risiko, dass biometrische Analysesysteme nach § 43a systematisch Personen mit bestimmten phänotypischen Merkmalen häufiger oder fehlerhafter erfassen könnten?

Antwort:

Dem TLfDI liegen hierzu keine konkreten Erkenntnisse vor. Maßgeblich hängt die Qualität solcher Systeme vom Algorithmus und den Testdaten ab. Siehe hierzu auch:

https://innen.hessen.de/sites/innen.hessen.de/files/2023-11/rvl_2023_-_praesentation_prof._dr._christian_rathgeb_-_16.11.2023.pdf .

Aufgrund der Vielzahl der Personen die in die Maßnahme einbezogen werden, kann auch eine geringe Fehlerquote dazu führen, dass eine nicht unerhebliche Anzahl der Menschen zu Unrecht von polizeilichen Maßnahmen erfasst wird.

Zu § 44

Frage § 115:

Wie bewerten Sie die Erweiterung der Rasterfahndungsschwelle auf KRITIS beziehungsweise Gemeinwesen? Ist das nach der Rechtsprechung zur präventiven Rasterfahndung verfassungsfest, oder erhöht es das Risiko, dass die Rasterfahndung in das Gefahrenvorfeld abrutscht?

Antwort:

Das Bundesverfassungsgericht hat in seiner Entscheidung vom 4. April 2006 festgestellt, dass eine „präventive polizeiliche Rasterfahndung mit dem Grundrecht auf informationelle Selbstbestimmung nur vereinbar ist, wenn eine konkrete Gefahr für hochrangige Rechtsgüter wie dem Bestand und die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person gegeben ist.“ (BVerfG, Beschluss vom 4. April 2006 – 1BvR 518/02 – 1. Leitsatz). Eine Rasterfahndung im Vorfeld der Gefahrenabwehr scheidet aus (BVerfG a.a.O.). Es bedarf also des Schutzes hochrangiger Rechtsgüter und des Vorliegens einer konkreten Gefahr. Das Fehlen einer konkreten Gefahr in § 44 SOG Mecklenburg-Vorpommern hatte das Bundesverfassungsgericht im Beschluss vom 9. Dezember 2022 – 1 BvR 1345/21 bemängelt. Aus diesem Grund sollte auch der Sachgüterschutz präzisiert sein und eng gefasst werden. Die Begründung zum Gesetzentwurf (S. 54) verweist auf § 34 PAG-E. Der Anwendungsbereich (z.B. „öffentliche Verwaltung“) ist hier aus Sicht des TLfDI im Verhältnis zur Eingriffsintensität der Maßnahme zu weit gefasst. § 46 Brandenburgisches Polizeigesetz ist deutlich enger gefasst („[...] soweit dies zur Abwehr einer konkreten Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person erforderlich ist (Rasterfahndung).“), ebenfalls auch § 31 Polizeigesetz des Landes Nordrhein-Westfalen („[...]soweit dies zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person erforderlich ist (Rasterfahndung)“).

Frage 116:

Welche Anforderungen an Datenkategorien, Kriterien, Drittschutz und Löschung müssten aus Ihrer Sicht zwingend gesetzlich verankert werden, um die Betroffenheit Unbeteiligter zu minimieren, und wären zusätzliche Kontrollmechanismen als Mindeststandard erforderlich?

Antwort:

§ 46 Abs. 1 Polizeiaufgabengesetz Bayern sieht beispielsweise einen Richtervorbehalt vor. Der Kontrollmechanismus ist dort höher angesetzt und somit verfahrensrechtlich strenger.

Mit freundlichen Grüßen

Tino Melzer