



TLT/5719/26/5

THUR. LANDTAG POST
21.05.2026 10:59
15440 12026SÄCHSISCHE DATENSCHUTZ- UND TRANSPARENZBEAUFTRAGTE
Postfach 11 01 32 | 01330 DresdenThüringer Landtag
Ausschuss für Inneres, Kommunales
und Landesentwicklung
Jürgen-Fuchs-Straße 1
99096 ErfurtDen Mitgliedern des
AfIKLThüringer Landtag
Z u s c h r i f t
8/557
zu Drs. 8/2478Ihr/-e Ansprechpartner/-in
Thomas MauersbergerDurchwahl
Telefon +49 351 85471-140
Telefax +49 351 85471-109

post@sdtb.sachsen.de*

Aktenzeichen
(bitte bei Antwort angeben)
4-2801/25/1-2026/12726Dresden,
20. Mai 2026**Zweites Gesetz zur Änderung des Polizeiaufgabengesetzes (Drucksache 8/2478) hier: Anhörungsverfahren gemäß § 79 der Geschäftsordnung des Thüringer Landtags**

Ihr Schreiben vom 17.3.2026; Zeichen: Drs. 8/2478-li

Sehr geehrte Damen und Herren,

vielen Dank für Ihr Schreiben vom 17. März 2026. Ihrer Bitte um Stellungnahme zum vorliegenden Entwurf eines Zweiten Gesetzes zur Änderung des Polizeiaufgabengesetzes (Drucksache 8/2478) komme ich gern nach. Angesichts der Komplexität des Gesetzgebungsvorhabens und des Umfangs des übersandten Fragenkatalogs bitte ich um Ihr Verständnis dafür, dass ich meine Stellungnahme auf ausgewählte Vorschriften des Entwurfs und wesentliche datenschutzrechtliche Aspekte beschränke. Eine erschöpfende Antwort auf alle die Fragen aus dem Fragenkatalog, die datenschutzrechtliche Bezüge aufweisen, ist mir leider nicht möglich; ich weise in meinen Ausführungen zu einzelnen Normen auf einschlägige Fragen hin.

Ganz allgemein möchte ich darauf hinweisen, dass im modernen und zunehmend digitale Anwendungen umfassenden Polizeirecht aus verfassungsrechtlicher Perspektive eine ganzheitliche Betrachtung der Befugnisse und ihrer Folgen zwingend ist. Einzelne Eingriffsbefugnisse dürfen nicht isoliert, sondern müssen vielmehr (auch) im Zusammenhang mit Befugnissen zur Speicherung und zur zweckändernden Verarbeitung der erhobenen Daten gesehen und bewertet werden. Grundrechtseingriffe enden nicht nach Abschluss einer konkreten (Datenerhebungs-)Maßnahme, sondern setzen sich in der – auch zweckändernden – Weiterverarbeitung der erhobenen Daten fort. Sind schon Einzelmaßnahmen aufgrund ihrer Eingriffstiefe oder Streubreite von schwerwiegendem Charakter, gilt dies erst recht im Zusammenspiel mit unangemessenen Speicherfristen und kaum begrenzten Weiterverwendungsmöglichkeiten. In besonderem Maß gelten diese Überlegungen hinsichtlich der automatisierten Datenanalyse, in die nach § 40a des Entwurfs ohne Differenzierung nach Personengruppen sämtliche in verschiedenen eigenen automatisierten Verfahren der Thüringer Polizei gespeicherten personenbezogenen Daten (§ 40a Abs. 1) bzw. sämtliche Daten aus Vorgangs-

Hausanschrift:
Sächsische
Datenschutz- und
Transparenzbeauftragte
Maternistraße 17
01067 Dresden

www.datenschutz.sachsen.de

Verkehrsanbindung:
Zu erreichen mit den S-Bahn-
Linien S1 und S2 sowie den
Straßenbahnlinien 7, 10 und 12
(Haltestelle S-Bf. Freiburger
Straße)*Informationen über die
Verarbeitung Ihrer personen-
bezogenen Daten und zum
Zugang für verschlüsselte E-Mails
finden Sie im Internet unter
www.datenschutz.sachsen.de/
datenschutzerklaerung.html.

und Fallbearbeitungssystemen, aus elektronischen Ermittlungs- und Kriminalaktensystemen und aus Informations- und Fahndungssystemen der Thüringer Polizei (§ 40a Abs. 2) einbezogen werden sollen.

Soweit ich mich im Folgenden auf Rechtsvorschriften beziehe, ohne das Gesetz zu bezeichnen, handelt es sich um solche aus dem vorliegenden Entwurf zur Änderung des Thüringer Polizeiaufgabengesetzes (Artikel 1 des Gesetzentwurfs).

§ 18a – Datenübermittlungen in Fällen häuslicher Gewalt (vgl. Frage 27 aus dem Fragenkatalog)

§ 18a Absätze 3 und 4 sehen in Fällen häuslicher Gewalt Datenübermittlungen an eine geeignete Beratungsstelle (Abs. 3 zum mutmaßlichen Verursacher) bzw. an die regional zuständige Interventionsstelle für Opfer häuslicher Gewalt (Abs. 4 zur mutmaßlich gefährdeten Person) vor, ohne dass die betroffenen Personen einer solchen Übermittlung zustimmen müssten.

Die Übermittlung personenbezogener Daten aus polizeilicher Aufgabenerfüllung an externe Stellen, die nicht unmittelbar der Abwehr einer konkreten Gefahr dient, sehe ich grundsätzlich kritisch. Wie vage der Zusammenhang mit konkreter Gefahrenabwehr ist, zeigt sich in den die Empfänger treffenden Löschpflichten, sofern die betroffenen Personen eine Beratung ablehnen. Mit Blick auf den Wesensgehalt des (Grund-)Rechts auf informationelle Selbstbestimmung – dieses umfasst die Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden, und daher grundsätzlich selbst über die Preisgabe und Verwendung persönlicher Daten zu bestimmen (vgl. BVerfGE 65, 1 <42 f.>; 67, 100 <143>) – wäre ein Festhalten an der bisherigen Rechtslage, wonach eine Übermittlung an Beratungsstellen nur mit Zustimmung der betroffenen Personen erfolgen darf, vorzugswürdig.

§ 21 Videoüberwachung in Gewahrsamseinrichtungen (vgl. Frage 29)

Die in § 21 Abs. 4 vorgesehene Videoüberwachung von polizeilichen Gewahrsamseinrichtungen begegnet hinsichtlich Bestimmtheit und Normenklarheit Bedenken. Nicht eindeutig ist zunächst, ob der Begriff der polizeilichen Gewahrsamseinrichtung auch einzelne Gewahrsamszellen umfasst. Während andere Landesgesetze zwischen Gewahrsamseinrichtung und Gewahrsamszellen – auch hinsichtlich der Eingriffsschwelle – differenzieren (§ 25 Abs. 1 SächsPVDG) und das Thüringer Landesrecht im Bereich des Justizvollzugs eine solche Unterscheidung vornimmt (§§ 32, 33 ThürJVollzDSG), spricht der Entwurf nur von „Gewahrsamseinrichtung“, legt aber in der Begründung nahe, dass auch einzelne Zellen erfasst sein sollen (S. 33).

Nicht nachvollziehbar ist die hinsichtlich der Anwendungsvoraussetzungen vorgesehene Gleichsetzung von weniger eingreifender (Live-)Bildübertragung und der schwerer wiegenden Bildaufzeichnung. Die unterschiedlichen Eingriffstiefen der Maßnahmen erfordern unterschiedliche Eingriffsschwellen, wobei die Befugnis zu Bildaufzeichnungen grundsätzlich an strengere Voraussetzungen zu knüpfen wäre. Das Thüringer Recht sieht eine Differenzierung zwischen Bildübertragung und -aufzeichnung im Freiheitsentzug bereits in §§ 33, 34 ThürJVollzDSG vor.



Fraglich ist überdies, ob eine Bildaufzeichnung zum Schutz von Personen überhaupt erforderlich ist. Mit Blick auf die räumliche Integration der Gewahrsamseinrichtung in eine polizeiliche Dienststelle, wird einer im Rahmen der Bildübertragung erkannten Gefahr unmittelbar durch den Einsatz von Bediensteten zu begegnen sei. Eine Bildaufzeichnung, die laut Begründung vorrangig der Beweismittelsicherung – also gerade nicht der Prävention – dienen soll (S. 33), wird in der Praxis regelmäßig auf strafprozessuale Vorschriften gestützt werden können, sofern ein Anfangsverdacht für eine strafbare Handlung (Sachbeschädigung, Körperverletzung) vorliegt. Das SächsPVDG verzichtet gänzlich auf eine Befugnis zur präventiven Bildaufzeichnung in polizeilichen Gewahrsamseinrichtungen (§ 25 SächsPVDG erlaubt lediglich die Bildübertragung).

Keine grundsätzlichen Bedenken bestehen gegen eine automatische Auswertung von Bildern im Rahmen der Bildübertragung (die freilich eine logische Sekunde der Aufzeichnung für den Prozess der automatischen Auswertung voraussetzt, wobei ich eine solche Verarbeitung nicht als Bildaufzeichnung im Sinne des Entwurfs ansehen würde).

Die in Abs. 5 vorgesehene Speicherfrist von 30 Tagen für Bildaufzeichnungen halte ich für unverhältnismäßig. Unabhängig von den grundsätzlichen Bedenken gegen eine Bildaufzeichnung in polizeilichen Gewahrsamszellen (s.o.) ist kein Grund ersichtlich, aus dem Aufzeichnungen aus polizeilichem Gewahrsam mindestens 27 Tage länger als Aufzeichnungen aus dem Justizvollzug aufbewahrt werden müssten - § 34 Abs. 1 Satz 2 ThürJVollzDSG sieht eine unverzügliche bzw. eine Löschung spätestens nach 72 Stunden vor.

§ 33 Videoüberwachung des öffentlichen Raums (vgl. Fragen 45, 46)

Während ich die in § 33 Abs. 4 vorgesehene automatische Auswertung von Bildaufzeichnungen aus der Videoüberwachung öffentlich zugänglicher Orte mit Blick auf die Beschränkung auf das Erkennen von verdächtigen Verhaltensmustern für vertretbar halte – eine Identifizierung oder gar biometrische Echtzeit-Fernidentifizierung ist gerade nicht vorgesehen –, ist die Befugnis, öffentlich zugängliche Orte bereits dann optisch zu überwachen, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass dort Straftaten verabredet, vorbereitet oder verübt werden sollen (vgl. § 14), aus meiner Sicht unverhältnismäßig.

Die polizeiliche Videoüberwachung (einschließlich Bildaufzeichnung) öffentlich zugänglichen Raums stellt einen erheblichen Grundrechtseingriff dar. Eine solche Maßnahme zählt zu verdachtslosen Eingriffen mit großer Streubreite, bei denen zahlreiche Personen in den Wirkungsbereich einer Maßnahme einbezogen werden, die in keiner Beziehung zu einem konkreten Fehlverhalten stehen und den Eingriff durch ihr Verhalten nicht veranlasst haben, und die grundsätzlich eine hohe Eingriffsintensität aufweisen (vgl. BVerfG, Stattgebender Kammerbeschluss vom 23. Februar 2007 – 1 BvR 2368/06 –, BVerfGK 10, 330-340, Rn. 51 mwN).

Dass bereits die Annahme, dass an einem Ort Straftaten verabredet oder vorbereitet werden sollen, einen intensiven Eingriff in Grundrechte ganz überwiegend Unbeteiligter rechtfertigen kann, erscheint mir mehr als zweifelhaft. Die Verabredung einer Straftat (eine Begrenzung auf schwere oder besonders schwere Straftaten enthält das Gesetz nicht, erfasst sind also auch Bagatelldelikte) ist weit entfernt von einer konkreten Rechtsgutgefährdung.

Angesichts der Eingriffstiefe der Maßnahme und der eingriffsverstärkenden einmonatigen Speicherfrist sähe ich eine höhere Eingriffsschwelle als unbedingt geboten an. Das

SächsPVDG sieht im Vergleich zur Regelung des § 33 ThürPAG eine Videoüberwachung von Kriminalitätsschwerpunkten nur dann vor, wenn auf den betreffenden öffentlichen Straßen, Wegen oder Plätzen nach polizeilich dokumentierten Tatsachen die Kriminalitätsbelastung gegenüber der des Gemeindegebiets deutlich erhöht ist und Tatsachen die Annahme rechtfertigen, dass dort künftig Straftaten begangen werden, durch die Personen, Sach- oder Vermögenswerte gefährdet werden (§ 57 Abs. 3 Nr. 2 SächsPVDG).

Die – leider nur – in der Begründung anklingende Beschränkung auf die Nutzung aus-
trainierter, statischer KI-Systeme sehe ich positiv. Der Ausschluss selbstlernender Systeme gewährleistet die Nachvollziehbarkeit der Ergebnisse der automatisierten Auswertung. Zugleich wird, auch das wird in der Begründung erwähnt, verhindert, dass die polizeilichen Daten (ganz überwiegend rechtstreu agierender Personen, s.o.) zum Training des Systems verwendet werden und in diesem verbleiben.

§ 34 Besondere Mittel der Datenerhebungen (vgl. Fragen 56 und 59)

Der Entwurf sieht in § 34, aber auch in anderen Befugnisnormen eine Änderung der Formulierung hinsichtlich der zu schützenden Rechtsgüter vor, wobei die bisherige Eingriffsschwelle der Abwehr einer gemeinen Gefahr für Sachen durch die Abwehr einer Gefahr „für Anlagen der kritischen Infrastruktur oder sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen“ ersetzt werden soll. Die Begründung verweist auf eine in ständiger Rechtsprechung des Bundesverfassungsgerichts erfolgende Verwendung des Begriffs der Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen (S. 39), die künftig neben bzw. zusätzlich („oder“) zu Anlagen der kritischen Infrastruktur erfasst sein sollen. Als Beispiel einer solchen Anlage wird „die öffentliche Verwaltung“ erwähnt.

Das Bundesverfassungsgericht nennt „wesentliche Infrastruktureinrichtungen oder sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen“ als Beispiele für Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist und fordert ein enges Verständnis. (vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 –, BVerfGE 162, 1-178, Rn. 243). Das heißt, dass auch „sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen“ Sachen bzw. Anlagen von bedeutendem Wert sein müssen, deren Erhaltung im öffentlichen Interesse geboten ist. Inwieweit hier „die öffentliche Verwaltung“ erfasst sein soll, ist fraglich.

Das Risiko einer Zunahme polizeilicher Maßnahmen auch bei gewaltfreien Protesten im Umfeld von KRITIS-Einrichtungen sehe ich als nicht erheblich an, soweit die Polizei – die an Gesetz und Recht gebunden ist – die Befugnisnormen verfassungskonform anwendet. Neben einer geänderten Beschreibung des polizeilichen Schutzguts tritt nach wie vor die Voraussetzung des Vorliegens einer (konkreten) Gefahr. Vorausgesetzt wird eine Sachlage, die bei ungehindertem Ablauf des objektiv zu erwartenden Geschehens im Einzelfall in absehbarer Zeit mit hinreichender Wahrscheinlichkeit zu einer Verletzung eines polizeilichen Schutzguts führt (vgl. BVerfG, Urteil vom 26. April 2022 – 1 BvR 1619/17 –, BVerfGE 162, 1-178, Rn. 158). Eine solche Sachlage dürfte bei gewaltfreien Protesten oder Streiks regelmäßig nicht vorliegen. Allein die räumliche Nähe zu KRITIS-Einrichtungen rechtfertigte dann keine deren konkrete Gefährdung voraussetzende Maßnahmen.

§ 38 Nutzung von Drohnen (vgl. Frage 87)

Soweit der Einsatz von Drohnen auch für die Bildübertragung und -aufzeichnung bei Veranstaltungen und Ansammlungen nach § 33 Abs. 1 erlaubt werden soll, sieht der Entwurf vor, dass die Offenheit der Maßnahme gewahrt bleiben muss. Es liegt in der Verantwortung der Polizei, dieses Gebot in der Praxis so umzusetzen, dass die von der Überwachung betroffenen Personen die Überwachung ohne Weiteres erkennen können. Bei einer solchen Umsetzung bestünden gegen den Einsatz von Drohnen keine durchgreifenden Bedenken.

§ 39 Zweckbindung, HyDaNe, Kennzeichnung (vgl. Fragen 90, 91)

§ 39 legt fest, für welche Zwecke die Polizei im Rahmen ihrer Aufgabenerfüllung erhobene Daten (weiter-)verarbeiten darf.

Absatz 1 betrifft dabei die Bearbeitung des der ursprünglichen Datenerhebung zugrundeliegenden Vorgangs („dieselbe“ Aufgabe und „dieselben“ Rechtsgüter bzw. Straftaten), Absatz 2 die Verwendung für andere Vorgänge, also die verfahrensübergreifende bzw. die vom Ursprungsverfahren unabhängige Nutzung. Letztere soll nur unter Beachtung des Grundsatzes der hypothetischen Datenneuerhebung (HyDaNe) zulässig sein. Danach muss die neue Nutzung der Daten dem Schutz von Rechtsgütern oder der Aufdeckung von Straftaten eines solchen Gewichts dienen, die verfassungsrechtlich ihre Neuerhebung mit vergleichbar schwerwiegenden Mitteln rechtfertigen könnten. Eine konkretisierte Gefahrenlage wie bei der Datenerhebung ist demgegenüber grundsätzlich nicht erneut zu verlangen; erforderlich aber auch ausreichend ist in der Regel das Vorliegen eines konkreten Ermittlungsansatzes (BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, BVerfGE 141, 220-378 (LT 1-3)).

Das Bundesverfassungsgericht hat festgestellt, dass auch im Falle einer zweckwahren Weiterverarbeitung die erhobenen Daten grundsätzlich zu löschen sind, nachdem der unmittelbare Anlassfall abgeschlossen und damit der der Erhebungsmaßnahme zugrundeliegende konkrete Zweck erfüllt ist. Danach ist eine zweckwahrende Verarbeitung nicht mehr zulässig (BVerfG, Urteil vom 1. Oktober 2024 – 1 BvR 1160/19 –, BVerfGE 169, 332-413, Rn. 141). Diese Vorgaben betreffen die zweckwahrende Verarbeitung nach § 39 Abs. 1.

Ein Absehen von einer Löschung über den unmittelbaren Anlassfall hinaus kommt nur in Betracht, soweit sich aus den Daten - sei es aus ihnen selbst, sei es in Verbindung mit weiteren Kenntnissen der Behörde - zwischenzeitlich ein konkreter Ermittlungsansatz ergeben hat (vgl. BVerfGE 141, 220 <322 f. Rn. 270>) und damit die Voraussetzungen einer zweckändernden Nutzung vorliegen (BVerfG, Urteil vom 1. Oktober 2024 – 1 BvR 1160/19 –, BVerfGE 169, 332-413, Rn. 141). Dieser Befund des Bundesverfassungsgerichts bezieht sich auf die zweckändernde Weiterverarbeitung nach dem HyDaNe-Grundsatz. § 39 Abs. 2 setzt diese Vorgaben um.

Das Risiko einer „Datenentgrenzung“ sehe ich nicht als erheblich an, denn die Voraussetzung des konkreten Ermittlungsansatzes für eine zweckändernde Weiterverarbeitung steht einer grenzenlosen Verwendung für andere oder gar noch nicht absehbare Verfahren entgegen.

Liegt kein konkreter Ermittlungsansatz vor, kann dementsprechend auch eine Speicherung personenbezogener Daten aus einem Vorgang für künftige, aktuell noch nicht absehbare Verwendungen (vorsorgende Speicherung) nicht auf § 39 Abs. 2 gestützt werden.

Absatz 6, der eine Ausnahme bzw. Suspendierung der Kennzeichnungspflicht nach Absatz 5 vorsieht, gefährdet im Fall seiner Anwendung die Einhaltung des nach Absatz 2 zwingend zu beachtenden HyDaNe-Grundsatzes, dessen Umsetzung – durch die jeweilige explizite Bezugnahme auf § 39 – zwingende Voraussetzung für die Anwendung bestimmter Weiterverarbeitungsbefugnisse ist (z.B. die automatisierte Datenanalyse nach § 40a). Ohne Kennzeichnung der Daten, die nach Absatz 5 auch die Erhebungsmittel und die betroffenen Rechtsgüter bzw. Straftaten umfasst, ist ein Vergleich im Sinne von § 9 Abs. 2 Satz 1 Nr. 1 kaum vorstellbar. Das bedeutet auch, dass ohne Kennzeichnung und daraus resultierende Vergleichsmöglichkeit die automatisierte Datenanalyse nach § 40a unzulässig ist, solange eine Kennzeichnung nicht erfolgt.

§ 40 Zweckändernde Weiterverarbeitung

Die vorgesehenen Änderungen des § 40 ThürPAG sind auf den ersten Blick geringfügig, erweisen sich bei genauerer Betrachtung m.E. aber als problematisch. In den Absätzen 1, 2 und 3 sollen die dort vorgesehenen Weiterverarbeitungsbefugnisse künftig (nur) „nach Maßgabe des § 39“ Anwendung finden.

§ 39 aber begrenzt eine Weiterverarbeitung auf die konkrete Vorgangsbearbeitung (§ 39 Abs. 1) sowie die verfahrensübergreifende Verwendung, sofern für die neue Verwendung „im Einzelfall konkreten Ermittlungsansätze“ vorliegen (Abs. 2), s.o.

Eine nach Absatz 1 zulässige Weiterverarbeitung für Zwecke der zeitlich befristeten Dokumentation oder zur Vorgangsverwaltung (diese dienen nicht der Gefahrenabwehr und stellen genau genommen eine zweckändernde Weiterverarbeitung dar) „nach Maßgabe des § 39“ ist kaum vorstellbar (Ausnahme: § 39 Abs. 4, aber dieser ließe dann nur eine Weiterverarbeitung der Grunddaten für Zwecke der zeitlich befristeten Dokumentation oder zur Vorgangsverwaltung nach § 40 Abs. 1 zu).

Die vorsorgende Speicherung nach § 40 Abs. 2 ThürPAG ist mit der Voraussetzung eines „im Einzelfall konkreten Ermittlungsansatzes“ im Sinne von § 39 Abs. 2 Nr. 2 ebenfalls nicht vereinbar. Grundlage der Speicherung für künftige Zwecke ist gerade nicht ein aktuell konkreter Ermittlungsansatz, sondern die – auf einer Negativprognose beruhenden – Wahrscheinlichkeit, dass die Daten in Zukunft für die Abwehr einer Gefahr oder die Verhütung oder Verfolgung einer Straftat erforderlich werden.

§ 40 Abs. 2 ThürPAG genügt m.E. auch im Übrigen nicht den verfassungsrechtlichen Vorgaben an eine vorsorgende Speicherung, die eine Zweckänderung darstellt, an eine eindeutig erkennbare Zweckbestimmung geknüpft sein muss und gewissen Anforderungen an die Eingriffsschwellen, hier in Form von Speicherschwelen, genügen muss (BVerfG, Urteil vom 1. Oktober 2024 – 1 BvR 1160/19 –, BVerfGE 169, 332-413, Rn. 180). Zwar betraf die Entscheidung des Bundesverfassungsgerichts vom 1. Oktober 2024 Vorschriften des BKAG und dort mit § 18 Abs. 1 Nr. 2 BKAG die vorsorgende Speicherung von Beschuldigten im polizeilichen Informationsverbund; die Ausführungen des Gerichts zur verfassungsrechtlichen Notwendigkeit von erkennbarer Zweckbestimmung



und bestimmten Eingriffs- bzw. Speicherschwelen sind aber ohne Weiteres auf Speicherungen einer Landespolizei in landespolizeilichen Informationssystemen übertragbar. § 40 Abs. 2 enthält weder eine eindeutig erkennbare Zweckbestimmung – die Vorschrift stellt lediglich undifferenziert auf die allgemeine polizeiliche Aufgabe der Gefahrenabwehr nach § 2 Abs. 1 ThürPAG ab – noch wird, jedenfalls hinsichtlich Verurteilter und Beschuldigter, eine Speicherschwelle bestimmt. Erforderlich wäre das Bestehen einer hinreichenden Wahrscheinlichkeit dafür, dass die vorsorgend gespeicherten Daten zur Erfüllung der mit der Speicherung letztlich verfolgten Zwecke benötigt werden (vgl. BVerfG, Urteil vom 1. Oktober 2024 – 1 BvR 1160/19 –, BVerfGE 169, 332-413, Rn. 185). Also eine sog. **Negativprognose**. Während § 40 Abs. 2 Nr. 3 und 4 ThürPAG für Verdächtige und Anlasspersonen eine Prognose fordert, fehlt dies bei Verurteilten und Beschuldigten. Die Einbeziehung von § 39 (s.o., „nach Maßgabe von § 39“) vermag den Mangel einer fehlenden Negativprognose nicht zu heilen; § 39 steht einer vorsorgenden Speicherung ohne konkreten Ermittlungsansatz prinzipiell entgegen (s.o.).

Auch die vorsorgende Speicherung von Angaben zu Personen nach Absatz 3 ist „nach Maßgabe des § 39“ nicht möglich, da eine vorsorgende Speicherung gerade nicht im laufenden Ursprungsvorgang (§ 39 Abs. 1) erfolgen soll oder einen im Einzelfall konkreten Ermittlungsansatz voraussetzt (§ 39 Abs. 2), s.o.

§ 40 Abs. 6 Satz 1 ThürPAG regelt den sog. Mitzieheffekt, der nach den Ausführungen des Bundesverfassungsgerichts in seiner Entscheidung vom 1. Oktober 2026 zur Erforderlichkeit der gesetzlichen Regelung einer angemessenen Speicherdauer (vgl. BVerfG, Urteil vom 1. Oktober 2024 – 1 BvR 1160/19 –, BVerfGE 169, 332-413, Rn. 187, 188, 189) verfassungsrechtlich kaum noch zu rechtfertigen ist. Besonderen Umständen kann im Einzelfall über die Anordnung der weiteren Speicherung auch nach Ablauf der Aussonderungsprüffrist hinaus Rechnung getragen werden.

Eine Überarbeitung der Änderungen in § 40 wäre für die Aufgabenerfüllung der Polizei m.E. zwingend erforderlich und läge in erster Linie in deren eigenem Interesse.

§ 40a Anlassbezogene automatisierte Datenanalyse (vgl. Fragen 94, 96, 98, 100)

§ 40a soll die anlassbezogene automatisierte Datenanalyse erlauben, wobei Absatz 1 eine weiter gefasste, eingriffsintensivere Verarbeitung vorsieht als Absatz 2, der die für Zusammenführung und Auswertung vorgesehenen Datenbestände bzw. -quellen (geringfügig) begrenzt. Der Begriff der automatisierten Datenanalyse taucht lediglich in der Überschrift auf, findet im Wortlaut der Vorschrift aber keine Verwendung. Nach dem Text darf die Polizei Daten „automatisiert zusammenführen und darauf bezogen weitere nach diesem Gesetz oder besonderen Rechtsvorschriften erhobene personenbezogene Daten verarbeiten“. Dass sich hinter dieser Formulierung eine automatisierte Datenanalyse verbirgt, ist kaum erkennbar. Wie ein „automatisiertes Zusammenführen“ technisch vorzustattgehen soll, ist unklar. Nach meinem Verständnis erfolgt eine automatisierte Datenanalyse in zwei Schritten: zunächst sind Datenbestände zu bestimmen bzw. auszuwählen, die zum Zweck der später anschließenden Analyse „zusammengeführt“ werden. Dieser „zusammengeführte“ Datenbestand wird dann nach bestimmten Suchparametern automatisiert analysiert. Wenn aber bereits das Zusammenführen von Daten automatisiert erfolgt, würde dies nach meinem Verständnis bedeuten, dass die automatisierte Anwendung sich stets auf den gesamten polizeilichen Datenbestand erstrecken würde

bzw. müsste, aus dem Daten „automatisiert zusammengeführt“ werden. Dies stünde allerdings in Widerspruch zu den in Abs. 1 und Abs. 2 vorgesehenen (geringfügigen) Begrenzungen der einzubeziehenden Datenbestände.

Es ist unklar, welches Verständnis des automatisierten Analyseverfahrens der Vorschrift insgesamt zugrunde liegt. Die in der Überschrift erwähnte Anlassbezogenheit, die Befugnis zum Zusammenführen und das Bestehen einer Gefahr für eines der in Abs. 1 Satz 1 genannten Rechtsgüter bzw. eine auf tatsächlichen Anhaltspunkten beruhende gewisse Wahrscheinlichkeit bevorstehender Straftaten (Abs. 2) legen nahe, dass bereits das Zusammenführen von Daten bei jeder einzelnen Anwendung der Maßnahme von Neuem erfolgt. Dies wäre insofern zu begrüßen, als Datenbestände, die zusammengeführt werden sollen, im Einzelfall passgenau auf den „Anlass bezogen“ ausgewählt werden könnten (im Wortlaut ist eine solche Auswahl insofern angelegt, als die Datenverarbeitungen zulässig sein sollen, „soweit“ dies für die Abwehr der Gefahr erforderlich ist) und eine überschießende Verarbeitung personenbezogener Daten vermieden würde.

Ein anlass- oder vorgangsbezogenes Zusammenführen von im Einzelfall relevanten Datenbeständen mit einer erst daran anschließenden Analyse dieser zusammengeführten Daten wäre wesentlich grundrechtsschonender als eine „parallele Datenhaltung“ der Polizei auf einer permanent bestückten Analyseplattform, auf der laufend der (nahezu) komplette Datenbestand der Polizei gespiegelt würde, oder der automatisierte „Durchgriff“ auf den (nahezu) gesamten aktuellen Originaldatenbestand der Polizei (s.o.). Dies gilt umso mehr, als die Entwurfsvorschrift keine Differenzierung nach einzubeziehenden Personengruppen vorsieht.

Der Entwurf der Sächsischen Staatsregierung für das Sächsische Polizeivollzugsdienstgesetz geht erkennbar und klar von einer nur temporär und eben „anlassbezogen“ befüllten Analyseplattform aus. Konsequenterweise wird im Gesetzentwurf eine Löschverpflichtung für die auf der Analyseplattform zusammengeführten Daten vorgesehen (vgl. § 62a Abs. 7 des Gesetzentwurfs der Sächsischen Staatsregierung zum SächsPVDG, LT-Drs. 8/6142).

§ 40a enthält zu diesem Punkt nichts Erhellendes. Rechtsanwender und Betroffene können nicht erkennen, wie nach Abschluss der Maßnahme mit den zusammengeführten und analysierten Daten verfahren werden soll, die nicht als neue Erkenntnisse in den konkreten und für die Durchführung der Maßnahme ursächlichen Vorgang übernommen werden.

Während der Ausschluss der Verwendung selbstlernender Systeme und die Beschränkung der einzubeziehenden Datenbestände auf eigene (landespolizeiliche) automatisierte Verfahren eine gewisse eingriffsmildernde Wirkung entfalten, wirkt sich der bereits erwähnte Mangel an Differenzierung nach Personengruppen, deren Daten in die Analyse einbezogen werden können, in § 40a eingriffsverstärkend aus. Tatsächlich ist im Ergebnis der Datenbestand, der bei Maßnahmen nach Abs. 1 und Abs. 2 analysiert werden kann, immens. Nach der Vorschrift werden bei Maßnahmen nach Abs. 1 oder 2 sämtliche Personen in die Analyse einbezogen, zu denen in den „Datenquellbeständen“ (automatisierte Verfahren der Thüringer Polizei und, nach Abs. 1, ggf. zusätzlich händisch erhobene zusätzliche Daten) Daten gespeichert werden. Damit sind regelmäßig eine Vielzahl von sich rechtstreu verhaltenden Personen betroffen (Anzeigeerstatter, Hinweisgeber, Geschädigte, Vertreter, Zeugen usw.). Bereits die in Abs. 3 Satz 1 Nr. 1 bis 3 genannten Verfahren enthalten vermutlich hunderttausende personenbezogene Datensätze. Der Grundrechtseingriff gewinnt aber an Gewicht, wenn Suchvorgänge nicht auf näher umschreibbare Personen ausgerichtet sind und keine sachliche Verbindung zwischen dem



gefährdeten Rechtsgut und den von der automatisierten Anwendung Betroffenen vorausgesetzt wird; es fehlt dann jede tatsächengestützte Verbindung zu einer konkret verantwortlichen Person (vgl. BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19 –, BVerfGE 165, 363-442, Rn. 94).

Kritisch ist in diesem Zusammenhang auch der Umstand zu sehen, dass Daten bestimmter Personengruppen nur mit Einwilligung der Betroffenen in den Informationssystemen der Polizei gespeichert werden dürfen (vgl. § 40 Abs. 3 ThürPAG). Es ist zu bezweifeln, dass die Einwilligung sich auch auf die Verwendung der Daten in einer automatisierten Datenanalyse bezieht bzw. die Betroffenen vor Abgabe ihrer Einwilligung über derartige Verarbeitungen informiert wurden.

Die Vorschrift enthält keinerlei Beschreibung oder Anforderung an die eingesetzten Verfahren, ebenso fehlt ein Gebot, nähere Bestimmungen in einer Verwaltungsvorschrift zu treffen. Angesichts der Risiken, die mit dem Einsatz neuer Technologien und nur begrenzt nachvollziehbarer Datenverarbeitungen verbunden sind, halte ich die Formulierung, dass Daten „weiterverarbeitet“ werden dürfen, für viel zu unbestimmt (s.o.). Die im Entwurf enthaltene Vorgabe, dass die Anzeige der Ergebnisse technisch auf mit den Suchparametern übereinstimmende Treffer zu beschränken ist – die allerdings auch nur für Analysen nach Abs. 2 gilt (!), – ist in diesem Zusammenhang nicht ausreichend. Ohne eine Begrenzung der Suchparameter läuft eine Begrenzung der Anzeige der Ergebnisse, die sich auf Suchparameter bezieht, ins Leere.

Um die Eingriffsintensität der Maßnahme zu reduzieren, wären daher bereits einschränkende Vorgaben für Suchparameter geboten. Zu diesem Punkt führt das Bundesverfassungsgericht aus: „Das Eingriffsgewicht erhöht sich insbesondere, wenn die Datenanalyse oder -auswertung nicht auf einem Suchbegriff, jedenfalls nicht auf einem auf den bislang erkennbaren Sachverhalt bezogenen Suchbegriff gründet, sondern darauf zielt, allein statistische Auffälligkeiten in den Datenmengen zu entdecken, die darüber hinaus (automatisiert) in weiteren Abgleichsschritten mit bestimmten Datenbeständen verknüpft werden und so zu weiteren Informationen führen können, nach denen zu suchen die Polizei zuvor keinen Anlass hatte“ (BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19 –, BVerfGE 165, 363-442, Rn. 93). Die „Anlassbezogenheit“ der Maßnahme sollte sich im ausdrücklichen Gebot der Verwendung von „anlassbezogenen Suchbegriffen“ widerspiegeln (vgl. § 62a Abs. 3 des Gesetzentwurfs der Sächsischen Staatsregierung zum SächsPVDG, LT-Drs. 8/6142).

Angesichts der Einordnung der automatisierten Datenanalyse als schwerwiegender Eingriff in die informationelle Selbstbestimmung der Betroffenen, der nur unter den engen Voraussetzungen zu rechtfertigen ist, wie sie allgemein für eingriffsintensive heimliche Überwachungsmaßnahmen gelten (BVerfG, a.a.O., Rn. 104), ist nicht ohne Weiteres nachvollziehbar, weshalb für Maßnahmen nach § 40a weder ein Richtervorbehalt noch eine Benachrichtigungspflicht vorgesehen sind, die für eingriffsintensive heimliche Überwachungsmaßnahmen mittlerweile Standard ist. Mit Blick auf den Umfang der Datenbestände, die für Maßnahmen nach § 40a Abs. 1 und 2 genutzt werden dürfen, und das weitgehende Fehlen eingriffsmildernder Vorkehrungen, müssen auch Maßnahmen nach § 40a als schwerwiegende Eingriffe in die informationelle Selbstbestimmung der Betroffenen angesehen werden.

Soweit die Anordnungsbefugnis für Maßnahmen nach Abs. 2 nur besonderen Führungspersonen zugewiesen werden soll (nach § 40a Abs. 2 Satz 3 soll für Maßnahmen nach

Abs. 2 Satz 1 § 34 Abs. 5 entsprechend gelten), ist unverständlich, weshalb für eingriffsintensivere Maßnahmen nach Absatz 1 keine Vorgaben hinsichtlich der Anordnungsbezugnis getroffen werden.

§ 40a ist hinsichtlich der Beschreibung der Maßnahme bzw. der konkreten Datenverarbeitung äußerst unbestimmt, weist an verschiedenen Punkten Unklarheiten auf und sieht kaum eingriffsmildernde Vorkehrungen vor, sodass die Verfassungsmäßigkeit der Vorschrift äußerst zweifelhaft ist.

§ 43a biometrischer Abgleich mit Internet (vgl. Fragen 106, 108)

Die Befugnis stellt einen erheblichen Eingriff in das Recht der Betroffenen auf informationelle Selbstbestimmung dar und erfasst Personen, deren Abbildungen und akustische Äußerungen im Internet zugänglich sind, in öffentlichen und in privaten Bereichen ungezielt.

Damit wird der gesamte öffentlich zugängliche Bereich des Internets praktisch zu einer Referenzdatenbank für polizeiliche Maßnahmen; mindestens Millionen von Menschen müssen dauerhaft gewärtigen, einem biometrischen Abgleich hinsichtlich ihrer im Internet zugänglichen Bilder und Tonaufzeichnungen mit polizeilichen Referenzdaten unterzogen zu werden. Die Streubreite der Maßnahme ist enorm.

Der Wortlaut der Norm wirft Fragen hinsichtlich Bestimmtheit und Normenklarheit auf, soweit die Polizei befugt sein soll, „öffentlich frei zugängliche personenbezogene biometrische Daten aus dem Internet (zu) erheben“. Lichtbilder, Videos und Tonaufzeichnungen sind zunächst keine biometrischen Daten; vielmehr können auf ihrer Grundlage biometrische Daten generiert werden (vgl. hierzu die Definition nach § 46 Nr. 12 BDSG: "biometrische Daten (sind) 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, insbesondere Gesichtsbilder oder daktyloskopische Daten"). Erst durch die technische Bearbeitung von Lichtbildern oder Stimmaufzeichnungen können biometrische Daten zur betroffenen Person erlangt werden. Eine Erhebung „öffentlich frei zugänglicher personenbezogener biometrischer Daten aus dem Internet“ dürfte daher praktisch ausgeschlossen sein.

Angeichts des Umstands, dass die Vorschrift keinerlei Einschränkung hinsichtlich des Datenbestandes „aus“ dem Internet vorsieht, mit dem der Polizei vorliegende Daten abgeglichen werden sollen, sondern eine ungezielte Suche ermöglicht, stellt sich die Frage, ob mit einer Maßnahme nach § 43a gegen das Verbot nach Art. 5 Abs. 1 Buchst. e KI-Verordnung verstoßen würde. Untersagt ist danach „das Inverkehrbringen, die Inbetriebnahme für diesen spezifischen Zweck oder die Verwendung von KI-Systemen, die Datenbanken zur Gesichtserkennung durch das ungezielte Auslesen von Gesichtsbildern aus dem Internet oder von Überwachungsaufnahmen erstellen oder erweitern“. Weil biometrische Merkmale für Abgleichszwecke eben nicht unmittelbar aus dem Internet erhoben werden können (s.o.), liegt die Annahme nahe, dass aus den im Internet zugänglichen Bildern zunächst, jedenfalls für eine „technische Sekunde“ und zur Ermöglichung eines biometrischen Abgleichs, eine Datenbank im Sinne von Art. 5 Abs. 1 Buchst. e KI-VO erstellt wird, die aus dem ungezielten – hier: hinsichtlich der in den Abgleich einzubeziehenden Bilder nicht begrenzten – Auslesen von Gesichtsbildern aus dem Internet

resultiert. Der Wissenschaftliche Dienst des Deutschen Bundestages stellt in einer rechtlichen Analyse vom 22. Januar 2026 hierzu fest, „dass ein automatisierter biometrischer Abgleich mit öffentlich zugänglichen Bildern zwingend den Aufbau einer Datenbank voraussetzt, die eine strukturierte Vorverarbeitung und effiziente Suche ermöglicht“ (<https://www.bundestag.de/resource/blob/1149732/EU-6-074-25-WD-5-105-25.pdf>, S. 16).

Zum Kriterium der „Ungezieltheit“ äußern sich die Leitlinien der Kommission zu verbotenen Praktiken der künstlichen Intelligenz gemäß der Verordnung (EU) 2024/1689. Danach bezieht sich das Merkmal „ungezielt“ auf „eine Technik, die wie ein ‚Staubsauger‘ funktioniert und so viele Daten und Informationen wie möglich aufnimmt, ohne auf speziell und individuell bestimmte Subjekte für das Auslesen abzielen. Durch das Auslesen werden Daten oder Inhalte wahllos ‚geerntet‘. Somit bedeutet der Begriff ‚ungezielt‘, dass kein besonderer Schwerpunkt auf bestimmte Einzelpersonen oder eine bestimmte Gruppe von Einzelpersonen gelegt wird.“ (<https://digital-strategy.ec.europa.eu/de/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act>, Rn. 228). Dies trifft auf § 43a zu.

Dem danach hohen Risiko eines Verstoßes gegen EU-Recht – und nationales Verfassungsrecht – könnte durch Vorgaben zur anlassbezogenen Eingrenzung des Datenbestandes begegnet werden, der aus dem Internet erhoben werden darf, um ihn biometrisch zu bearbeiten und zu Abgleichszwecken zu nutzen.

Datenschutzrechtlich problematisch ist auch die Fehleranfälligkeit von Systemen zur automatisierten Fernidentifizierung. Selbst bei einer außerordentlich geringen Fehlerquote wäre aufgrund der großen Menge an erfassten Personen die Zahl der von falsch-positiven Treffern sehr hoch, womit eine nicht geringe Wahrscheinlichkeit dafür anzunehmen ist, dass Personen aufgrund von automatisierten Falschbewertungen zu Unrecht eingriffsstarken polizeilichen Maßnahmen unterworfen werden können.

Äußerst kritisch sind im Übrigen – sowohl in verfassungsrechtlicher als auch in polizeifachlicher Hinsicht – auch Diskriminierungstendenzen bei Verfahren der automatisierten biometrischen Gesichtserkennung zu betrachten.

Danach bestehen starke Bedenken gegen Vereinbarkeit von § 43a mit EU-Recht (Art. 5 Abs. 1 Buchst. e KI-VO) und – vor allem im Hinblick auf die extreme Streubreite und die „Ungezieltheit“ der Maßnahme – mit deutschem Verfassungsrecht.

§ 45 Polizeiliche Zuverlässigkeitsüberprüfungen (vgl. Frage 120)

§ 45 regelt die polizeiliche Zuverlässigkeitsüberprüfungen bestimmter Personen. Während der Regelungsbedarf nachvollziehbar ist, ist nicht ersichtlich, weshalb die Vorschrift kaum grundrechtsschonende Bestimmungen enthält. Dies vor allem vor dem Hintergrund, dass Zuverlässigkeitsüberprüfungen nur entfernt Zusammenhänge mit der Abwehr konkreter Gefahren aufweisen, im Regelfall im Anwendungsbereich der DSGVO erfolgen dürften, mit der Erhebung von Daten bei Dritten einhergehen und § 45 eine Durchbrechung des Trennungsgebots bzgl. der Datenbestände von Polizei und Verfassungsschutzbehörden vorsieht – eine Erkenntnisquelle sollen nach § 45 Abs. 3 Satz 2 Nr. 3 auch Verfassungsschutzbehörden sein.

Fraglich ist daher, aus welchem Grund keine Zustimmung der Betroffenen vorgesehen ist. Nach dem Thüringer Sicherheitsüberprüfungsgesetz sind Sicherheitsüberprüfungen

nur zulässig, wenn die betroffene Person zugestimmt hat (§ 6 Abs. 2 ThürSÜG). § 45 Abs. 2 sieht hingegen lediglich eine Information vor, obwohl auch bei Zuverlässigkeitsüberprüfungen nach § 45 die Polizei Daten bei Dritten über die betroffene Person erhebt, die die Polizei für die unmittelbare Aufgabenerfüllung nicht erheben dürfte. Die betroffene Person setzt allerdings nicht durch ihr – Rechtsgüter gefährdendes - Verhalten eine polizeiliche Befassung mit ihr in Gang, sondern allein durch eine (angestrebte) legale (berufliche) Tätigkeit.

Mit Blick auf den Charakter der Vorschrift, der kaum als gefahrenabwehrend bezeichnet werden kann (s.o.), und den Anlass der Datenerhebung sowie die Durchbrechung des Trennungsgebots bezüglich der Datenverarbeitung von Polizei und Nachrichtendiensten sollte auch bestimmt werden, dass die zum Zweck der Zuverlässigkeitsüberprüfung erhobenen Daten nicht im operativ genutzten und der gesamten Polizei zugänglichen bzw. für umfangreiche automatisierte Datenanalysen nach § 40a nutzbaren Datenbestand gespeichert werden dürfen (vgl. § 6 Abs. 1 Satz 3 SächsPolZÜG); Absatz 6 setzt lediglich zeitliche Vorgaben für die Speicherung.

Für die Beantwortung eventueller Rückfragen stehe ich Ihnen gern zur Verfügung.

Mit freundlichen Grüßen



Dr. Juliane Hundert
Sächsische Datenschutz- und Transparenzbeauftragte