

THÜR. LANDTAG POST
03.06.2026 06:25

1707312026



TLT/5920/26/9



Deutsches Forschungsinstitut
für öffentliche Verwaltung

German Research Institute
for Public Administration

FÖV / Postfach 14 09 / 67324 Speyer

An den Thüringer Landtag

**Ausschuss für Inneres, Kommunales und
Landesentwicklung**

Jürgen-Fuchs-Straße 1
99096 Erfurt

Univ.-Prof. Dr. Mario Martini
Leiter des Themenbereichs »Digitale
Transformation im Rechtsstaat«

Telefon +49 89 6004-4372

E-Mail mario.martini@unibw.de

Webseite https://unibw.de/public_law/

**Den Mitgliedern des
AfIKL**

Thüringer Landtag
Z u s c h r i f t
8/587

zu Drs. 8/2478

1.6.2026

**Stellungnahme für den Ausschuss für Inneres, Kommunales und Landesentwicklung des
Thüringer Landtags zum Entwurf eines Gesetzes zur Änderung des Polizeiaufgabengesetzes
(Drucksache 8/2478)**

Sehr geehrter Herr Dr. König,
sehr geehrter Herr Dr. Hyckel,
sehr geehrter Herr Linse,
sehr geehrte Damen und Herren,

für das Vertrauen, das Sie mir mit der Einladung zur Stellungnahme entgegengebracht haben, danke ich Ihnen sehr. Die Anfrage erreichte mich zu einem Zeitpunkt, zu dem ich bereits eine große Vielzahl zeitgebundener Aufgaben übernommen hatte, die keinen Aufschub zulassen. Gerne hätte ich noch zahlreiche weitere Fragen beantwortet, musste mich aber notgedrungen auf das beschränken, was innerhalb der mir zur Verfügung stehenden Zeit möglich war.

An der Stellungnahme haben Dr. Anna Berry, Luci Haspinger und Tom Schuchort (Deutsches Forschungsinstitut für öffentliche Verwaltung) in sehr gelungener Weise mitgewirkt.

Wenn die Erwägungen und Überlegungen den Gesetzgebungsprozess bereichern, freut mich das.

Mit den besten Grüßen

Univ.-Prof. Dr. Mario Martini

A. Grundsätzliche Fragen	2
I. Frage 3	2
II. Frage 12	6
III. Frage 16	8
1. Verfassungsrechtliche Risiken	8
2. Anforderungen der KI-VO	9
a) Art. 5 Abs. 1 lit. h KI-VO (Biometrische Echtzeit-Fernidentifizierungssysteme)	9
b) Art. 5 Abs. 1 lit. e KI-VO (sog. Scraping)	10
c) Art. 6 KI-VO (Hochrisikosysteme)	10
B. Fachfragen zu einzelnen Normen	11
I. Zu § 11	11
Frage 20	11
II. Zu § 21	12
1. Frage 29	12
2. Frage 32	13
III. Zu § 33	14
Frage 42	14
IV. Zu § 38	16
Frage 87	16
a) Technische Besonderheiten von Drohnen	16
b) Rechtliche Schlussfolgerungen	18
V. Zu § 43a	19
1. Frage 106	19
2. Frage 112	20
3. Frage 113	21

A. Grundsätzliche Fragen

I. 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?

Gefahrenabwehr ist die Kernaufgabe der Polizei. Die klassische Gefahrenabwehr ist allerdings längst nicht mehr die gleiche, die sie noch im Jahr 1882 zur Zeit des Kreuzberg-Urteils des Preußischen Obergerichtspräsidenten war. Stetig verändern und optimieren neue technologische Möglichkeiten die Aufgaben polizeilichen Handelns grundlegend.

Frühe Formen datengetriebener Polizeiarbeit entstanden bereits mit dem Aufkommen der ersten Computer und mit den ersten digitalen polizeilichen Datenbanken der 1990er Jahre. Mit der technologischen Weiterentwicklung blieb die polizeiliche Arbeit daher nie stehen. Heute treiben vor allem Künstliche Intelligenz, ständig wachsende Datenbestände und der Schutz vor neuen Bedrohungslagen das Schwungrad der technologischen Vielfalt voran.

Bereits der EGMR betonte im Jahr 2010 zu Recht: Es stehe außer Frage, dass der wirksame Kampf gegen Verbrechen heute weitgehend vom Einsatz moderner wissenschaftlicher Techniken abhängt.¹ Der Einsatz KI-gestützter Datenauswertungstools, wie sie auch der Gesetzesentwurf vorsieht, markiert insoweit ein weiterentwickeltes neues Zeitalter datengetriebener Polizeiarbeit. Werkzeuge wie eine intelligente Videoüberwachung, eine automatisierte Kraftfahrzeugkennzeichenerkennung, der Einsatz von Drohnen, der automatisierte Datenabgleich oder ein nachträglicher biometrischer Internetabgleich sind Teil eines technologischen Wandels einer modernen und deutlich verstärkten datengestützten Polizeiarbeit.²

Dieser Fortschritt bringt zwei grundsätzlich gegensätzliche Strömungen hervor. Der Technikbegeisterung und Hoffnungen auf mehr Sicherheit sowie effizientere Kontrolle auf der einen Seite stehen dystopische Befürchtungen vor einer totalen staatlichen Überwachung mit umfassenden Persönlichkeitsprofilen gegenüber.

So sehr der zunehmende Einsatz datengetriebener Werkzeuge polizeilicher Arbeit und Ermittlungserfolge neue Spielräume eröffnet, so sehr täuscht die scheinbare Objektivität

¹ EGMR, NJOZ 2010, 696 (701).

² Dazu für den Kontext der Versammlungsbeobachtung bspw. bereits *Martini/Thiessen et al.*, Digitale Versammlungsbeobachtung, 2023, S. 16 ff.

algorithmischer Werkzeuge schnell über die fehlende Neutralität der Datengrundlagen hinweg. Rassistische Einstellungen oder vorurteilsbehaftete Sichtweisen einzelner Polizeibeschäftigter beeinflussen das polizeiliche Handeln heute bereits in der analogen Welt (z. B. Racial Profiling). Dieselben Verzerrungen fließen zwangsläufig in die Datenbasis einer datengestützt vorhersagenden Polizeiarbeit ein. Bestimmte Gruppen geraten in der Folge aufgrund ihrer Herkunft oder ihres sozioökonomischen Status stärker in den polizeilichen Fokus (Bias).³ Das kann im schlimmsten Fall einen datengetriebenen Teufelskreis in Gang bringen.

KI-Systeme sind ihrer Natur nach darauf ausgelegt, Muster und Zusammenhänge in Daten zu erkennen. Sie können Zusammenhänge detektieren, die ein Polizist bei manueller Datenauswertung nicht ohne Weiteres erkennen könnte. Das stärkt zwar einerseits die Sicherheit, erhöht aber andererseits das Risiko, Freiheitsrechte in einer unverhältnismäßigen Weise einzuschränken. Es sind daher Sicherheitsmechanismen geboten, die die Auswertungsmacht der Polizei rechtsstaatlich domestizieren. Das gilt nicht zuletzt im Hinblick auf das Risiko, dass unbeteiligte Dritte, die außerhalb der Gefahrensituation stehen, in das umfassendere Prüfraster des Algorithmus geraten und so zu einem „gläsernen Bürger“ mutieren.

Die Instrumente des Gesetzesentwurfs legen den Grundstein für eine Infrastruktur, die es ermöglicht, sensible Daten flächendeckend zu erfassen und zu analysieren. Unter einer autoritären Regierung lassen sich diese Mittel für Zwecke der Überwachung und Einschüchterung instrumentalisieren. Bestimmte Personengruppen und auch Unbeteiligte systematisch zu erfassen, kann im schlimmsten Fall den Nährboden für willkürliche Maßnahmen gegen Regimekritiker, Minderheiten oder politische Gegner legen. Dass es sich hierbei nicht bloß um ein hypothetisches Szenario handelt, zeigen insbesondere die Enthüllungen über die Spyware „Pegasus“ in verschiedenen europäischen Staaten mit autoritären Tendenzen: Die jeweiligen Regierungen setzten die Überwachungssoftware gezielt ein, um regierungskritische Stimmen auszuspähen, zu unterdrücken oder zu verleumden. Ungarns ehemalige Führung überwachte mit Pegasus bspw. Hunderte Journalisten, Menschenrechtsaktivisten und Oppositionspolitiker. Auch Polens Regierung nutzte die Software im Zuge ihrer autoritären Wende, um Hunderte Oppositioneller zu überwachen. Ein weiteres prominentes Negativbeispiel

³ Allgemein zu Bias *Braun Binder/Egli*, in: Martini/Wendehorst, KI-VO, 2. Aufl. 2026, Art. 10 Rn. 26 ff.

autoritären Datenmissbrauchs liefert China: ⁴ Das umfangreich ausgebaute chinesische Überwachungsnetzwerk soll Presseberichten zufolge nahezu alle öffentlichen Orte, bspw. Bahnhöfe und Parks, flächendeckend mit Kameras erfassen. Die hierbei verwendeten intelligenten Kamerasysteme sind in der Lage, zu registrieren, wenn Gruppen sich (spontan) versammeln, und können diese dann gezielt und lückenlos überwachen. Den virtuellen Augen des Systems bleibt in dieser Hinsicht kaum eine menschliche Handlung verborgen: Prall gefüllte Datensilos, komplexe Algorithmen und intelligente Videokameras bilden elementare Bausteine des autoritären Machterhalts.⁵ Das Regime opfert damit letztlich den Privatheitsschutz auf dem Altar der Doktrin unbedingten Fortschritts. Nicht zufällig bildete das chinesische Social-Scoring-System die Negativ-Blaupause für das Verbot aus Art. 5 Abs. 1 lit. c KI-VO.

Die Risiken großer Datenmacht und Datenanalysetechniken können sich auf allen Ebenen exekutivischer Handlungsmacht entfalten. Auch Deutschland liefert Beispiele für den Missbrauch polizeilicher Datenbestände: In Mecklenburg-Vorpommern griffen etwa Polizeibeamte wiederholt unrechtmäßig auf Polizeidatenbanken zu, um Minderjährige zu kontaktieren. In einigen Fällen kam es sogar zu sexuellen Belästigungen.⁶ Ebenfalls in Mecklenburg-Vorpommern soll die neonazistische Gruppierung „Nordkreuz“ über polizeiliche Dienstcomputer Listen mit rund 25.000 Namen und Daten politischer Gegner angelegt haben.⁷ Ab 2018 verschickte zudem eine unbekannte Person oder Gruppe unter dem Namen „NSU 2.0“ Drohmails, die sich vor allem gegen Menschen mit Migrationsgeschichte richteten. Kurz zuvor hatten Polizeibeamte, von denen einige dem rechtsextremen Spektrum zuzurechnen sein sollen, die persönlichen Daten der Betroffenen aus polizeilichen Datenbanken abgefragt.⁸ Die Vielzahl solcher Vorfälle macht deutlich, dass rechtswidrige Datenabfragen im Polizeialltag bei einer rechtsstaatlichen Analyse immer mitzudenken sind.

⁴ Dazu bspw. *Martini/Thiessen et al.* (Fn. 2), S. 14 f.

⁵ Dazu bspw. *Martini/Thiessen et al.* (Fn. 2), S. 14 f.

⁶ FAZ.net, Polizisten nutzen Daten, um minderjährige Mädchen zu kontaktieren, 8.6.2019, abrufbar unter <https://www.faz.net/aktuell/gesellschaft/kriminalitaet/polizisten-nutzten-daten-um-minderjaehrige-maedchen-zu-kontaktieren-16227841.html>.

⁷ Tagesspiegel, „Todeslisten“ von rechtsextremisten „Nordkreuz“ sammelte 25.000 Adressen politischer Gegner, 6.7.2019, abrufbar unter <https://www.tagesspiegel.de/politik/nordkreuz-sammelte-25000-adressen-politischer-gegner-6604876.html>.

⁸ Die ZEIT.de, LKA hat Informationen über 69 rechtsextreme Drohmails, 21.7.2020, <https://www.zeit.de/gesellschaft/zeitgeschehen/2020-07/nsu-2-0-drohmails-polizeirechner-hessen-datenabfrage>.

Die angestrebten technologischen Mittel zur Gefahrenabwehr tragen als staatliche Datenmacht ihrer Natur nach das Risiko eines späteren autoritären Missbrauchs in sich. Sie stehen für eine neue Spielart der datengetriebenen Polizeiarbeit. Gerade weil demokratischen Ordnungen politischer Wandel immanent ist und künftige Machtverhältnisse nicht zuverlässig vorhersehbar sind, ist es angezeigt, die Bewertung moderner Überwachungsbefugnisse nicht allein vom Vertrauen in die aktuelle Regierung abhängig zu machen. Der Rechtsstaat denkt staatliche Handlungsinstrumente immer auch vom Missbrauchsfall her. Die Furcht vor einem potenziellen Missbrauch dieser Datenmacht durch eine möglicherweise autoritäre thüringische Regierung, sei sie linksextrem, sei sie rechtsextrem, ist daher keineswegs unbegründet.

II. Frage 12

Der Gesetzentwurf sieht die Möglichkeit der Nutzung automatisierter Datenanalyseverfahren vor. Welche grundrechtlichen Risiken ergeben sich aus Ihrer Sicht für das Recht auf informationelle Selbstbestimmung, insbesondere im Hinblick auf die Zusammenführung großer Datenbestände und mögliche Profilbildungen?

Die zunehmende Erfassung von Daten aus verschiedensten Lebensbereichen und die lückenlose Sammlung von Informationen über längere Zeiträume beschwören ihrer Natur nach das Risiko herauf, einen gläsernen Bürger und eine staatliche Machtkonzentration hervorzubringen. Denn sie erhöhen die algorithmische Prognosefähigkeit, die in verdichtete Bewegungs-, Verhaltens- oder Beziehungsprofile von Personen münden kann. Diese Profile beruhen auf einem algorithmischen Hypothesen- und Mustererkennungsprozess, dessen technische Feinheiten sich von außen nur schwer bis gar nicht überprüfen lassen.⁹ Selbst anonymisierte oder pseudonymisierte Daten bergen im Gefolge vermeintlich harmloser Informationen, wie Ortsangaben, Alter oder Geschlecht, ein Reidentifikationsrisiko.¹⁰ Führt der Staat Datensätze aus öffentlich zugänglichen Registern, Portalen usw. zusammen, kann daraus im Ergebnis ein umfassendes Abbild individueller Merkmale und gesellschaftlicher Prozesse erwachsen, das im Extremfall umfassende Persönlichkeitsprofile sowie ein gesellschaftliches Gefühl polizeilicher Überwachung (sog. chilling effects) hervorbringt.

⁹ Vgl. EuGH ECLI:EU:C:2022:491 Rn. 58, 106.

¹⁰ Katko/Babaei-Beigi, MMR 2014, 360 (361).

Wie schon in seiner Mikrozensus-Entscheidung¹¹ betont das Bundesverfassungsgericht auch heute in ständiger Rechtsprechung den kategorialen verfassungsrechtlichen Schutz des Bürgers vor einer Katalogisierung.¹² Der Umstand, dass die intelligente Verknüpfung von Daten bislang irrelevanten oder nebensächlichen Informationen einen neuen Gehalt und neuen Stellenwert verleihen kann, zeigt die Grundrechtsintensität bei Datenerhebungen wie einer intelligenten Videoüberwachung und Videoauswertung auf öffentlichen Plätzen auf. Bereits die bloße Sammlung und Verknüpfung der Aufnahmen, die sich gezielt gegen einzelne Personen richtet, greift in die informationelle Selbstbestimmung ein.

Der Einsatz von KI-Modellen zur automatisierten Analyse solcher Daten steigert die Eingriffsintensität dieser Maßnahmen noch einmal zusätzlich. Je ausgereifter die Analysefähigkeiten des Systems sind, umso größer der Informationsgehalt und das grundrechtliche Risiko für die informationelle Selbstbestimmung. Selbst wenn die Polizei einen bisher lediglich manuell ausgeführten Vorgang automatisiert, ohne den Inhalt des Vorgangs substantiell zu verändern, erhöht dies bereits ihre Schlagkraft. Eine solche Automatisierung, wie sie etwa § 40a PAG-E vorsieht, wiegt deshalb besonders schwer und verlangt mit Blick auf das Gebot der Verhältnismäßigkeit eine umso strengere Rechtfertigung. Besonders wichtig sind dabei:

- hinreichend hohe Eingriffsschwellen für eingriffsintensive Datenanalysen,
- verpflichtende Kontrollkonzepte mit regelmäßigen Prüfungen durch die Datenschutzbehörden,
- spezifische Regelungen für lernende Systeme, die deren Einsatzvoraussetzungen und Kontrollanforderungen präzise festlegen,
- Transparenzvorgaben für private Software, die staatliche Nachvollziehbarkeit sicherstellen, und
- Investitionen in digitale Souveränität durch staatliche Eigenentwicklungen und Nutzung von KI-Reallaboren.¹³

¹¹ BVerfGE 27, 1 (6 ff.).

¹² BVerfGE 65, 1 (57); 115, 320 (351); BVerfG, ZD 2018, 578 (582).

¹³ Martini/Botta, Polizeiliche Datenanalyse mittels KI, DÖV 2025, 1033 (1044); Martini/Botta, „Sehende Steine“ statt „Kommissar Zufall“?, DÖV Blog 2026, blog.kohlhammer.de/doev/sehende-steine-statt-kommissar-zufall.

III. 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?

Moderne Bilderkennungstechnologien, wie sie etwa § 33 PAG-E¹⁴ vorsieht, sind der Rechtsordnung nicht grundsätzlich fremd. Das vorgesehene Analyseverfahren bewegt sich funktional in den Bahnen bekannter Überwachungsmechanismen, bei denen mit Hilfe künstlicher Intelligenz und vortrainierter Systeme eine Analyse anhand zuvor definierter Muster stattfindet, ohne dass hierbei notwendig eine biometrische Fernidentifizierung erfolgt.

Ein neues, sehr sensibles Kapitel polizeilicher Bilderkennungsmethoden schlägt demgegenüber § 43a PAG-E auf. Die Regelung versucht, die technischen Möglichkeiten nutzbar zu machen, die sich mit modernen Anwendungen wie Clearview verbinden. Dass sich die mutmaßliche RAF-Terroristin Daniela Klette mithilfe dieser Technologien hat ausfindig machen lassen,¹⁵ zeigt die technologischen Potenziale sehr deutlich auf. Nicht minder sensibel ist die Technologie aber. Denn sie hebt die Anonymität des Alltäglichen faktisch auf.¹⁶

1. Verfassungsrechtliche Risiken

Das Bundesverfassungsgericht hat bereits der herkömmlichen Videoüberwachung ein „breitenwirksames Gefahrenpotenzial“ zugeschrieben.¹⁷ Jede zusätzliche Stärkung staatlicher Überwachung erhöht das Risiko, dass Einschüchterungseffekte Grundrechtsträger daran hindern, ihre Freiheitsrechte auszuüben.¹⁸ Kommen intelligente Überwachungssysteme gleichzeitig an mehreren öffentlich zugänglichen Orten zum Einsatz und werden sie mit den verwendeten Analysetechniken verknüpft, erhöht das die Eingriffsintensität fühlbar.¹⁹ Es droht eine weitreichende Erfassung von Bewegungen und Lebensäußerungen auch solcher

¹⁴ Vergleichbare Regelungen finden sich auch in Art. 33 Abs. 5 BayPAG oder in § 44 Abs. 4 PolG BW.

¹⁵ Sueddeutsche.de, Wie viel Überwachung darf es sein?, 23.3.2024, abrufbar unter <https://www.sueddeutsche.de/wissen/gesichtserkennung-kuenstliche-intelligenz-raf-polizei-straftaeter-1.6475215?reduced=true>.

¹⁶ Dazu bereits Martini/Kemper, CR 2023, 341 ff. und 414 ff.

¹⁷ BVerfGE 141, 220 (268).

¹⁸ BVerfGE 115, 320 (354) m. w. N.

¹⁹ Petri, GSZ 2018, 144 (148).

Personen, die in keiner Beziehung zu einem konkreten Gefährdungsverhalten stehen, sondern lediglich durch Falsch-Positiv-Meldungen des Systems zu Unrecht oder gleichsam als Beifang in dessen Fokus geraten. Ein solches Vorgehen greift tief in das Recht auf informationelle Selbstbestimmung ein. Der Umfang und die Intensität der Bildanalyse verstärken die Intensität dieses Eingriffs weiter, da sich betroffene Personen in ihrem Verhalten beobachtet fühlen und dadurch von der Ausübung bestimmter Freiheitsrechte abgeschreckt werden können.

2. Anforderungen der KI-VO

Die KI-VO formuliert für biometrische Fernidentifizierungssysteme besondere Zulässigkeitsanforderungen. Sie versteht darunter KI-Systeme, die dem Zweck dienen, natürliche Personen ohne ihre aktive Einbeziehung in der Regel aus der Ferne durch Abgleich biometrischer Daten mit den in einer Referenzdatenbank gespeicherten biometrischen Daten zu identifizieren – und zwar unabhängig davon, welche Technologien, Verfahren oder Arten biometrischer Daten dazu Verwendung finden (ErwGr. 17 S. 1 KI-VO, Art. 3 Nr. 41 KI-VO).

§ 43a PAG-E setzt das Funktionsprinzip einer Fernidentifizierung paradigmatisch um: Die Polizei erhebt biometrische Daten aus dem Internet und gleicht diese automatisiert mit bereits vorhandenen biometrischen Daten zu Gesichtern und Stimmen ab, um Personen zu identifizieren.

a) Art. 5 Abs. 1 lit. h KI-VO (Biometrische Echtzeit-Fernidentifizierungssysteme)

Art. 5 Abs. 1 lit. h KI-VO untersagt den Einsatz biometrischer Echtzeit-Fernidentifizierungssysteme durch Strafverfolgungsbehörden grundsätzlich.²⁰ Wie der Wortlaut zu erkennen gibt, ist diese Regelung jedoch nur auf Echtzeit-Identifizierungen anwendbar, bei denen die Erfassung biometrischer Daten, deren Abgleich sowie die Identifizierung ohne erhebliche Verzögerung erfolgen.

Bei § 33 Abs. 4 S. 2 und 3 PAG-E fehlt es bereits an einer biometrischen Identifizierung i. S. d. Art. 3 Nr. 35 KI-VO.

²⁰ Wendehorst, in: Martini/Wendehorst, KI-VO, 2. Aufl. 2026, Art. 5 Rn. 190.

Im Falle des § 43a PAG-E erfolgt zwar eine biometrische Identifizierung. Diese geschieht jedoch nicht in Echtzeit: Der Wortlaut des § 43a PAG-E erfasst ausdrücklich nur „nachträgliche“ biometrische Abgleiche. Auch diese fällt daher nicht in den Anwendungsbereich des Art. 5 Abs. 1 lit. h KI-VO.

b) Art. 5 Abs. 1 lit. e KI-VO (sog. Scraping)

Auf das System des § 43a PAG-E findet allerdings die Verbotsnorm des Art. 5 Abs. 1 lit. e KI-VO Anwendung. Denn es gleicht „mittels einer automatisierten Anwendung zur Datenverarbeitung“ biometrische Daten mit öffentlich frei zugänglichen personenbezogenen Daten aus dem Internet ab. Soweit es sich um Gesichtsbilder²¹ aus dem Internet nach dem Vorbild von Clearview²² handelt, lässt der europäische Gesetzgeber dies bewusst nicht zu, soweit beim Auslesen künstliche Intelligenz zum Einsatz kommt (Art. 2 Abs. 1 i. V. m. Art. 3 Nr. 1 KI-VO). Denn eine solche Praktik beeinträchtigt die Privatsphäre und den Datenschutz Betroffener in unangemessener Weise. Darüber hinaus trägt sie dazu bei, ein Gefühl ständiger Beobachtung und Überwachung zu induzieren.

Scraping-Technologien setzen für den Abgleich typischerweise auf künstliche Intelligenz und die Erstellung einer Datenbank, um ihre Aufgabe angemessen erfüllen zu können. Technisch kann sich das auch als notwendig erweisen.²³ Weder der Gesetzestext noch die Begründung des Änderungsgesetzes machen deutlich, dass der Gesetzgeber den Einsatz künstlicher Intelligenz in diesem Verfahren ausschließt. Der Gesetzentwurf ist daher nach meiner Einschätzung in seiner jetzigen Form mit der KI-VO nicht vereinbar.

c) Art. 6 KI-VO (Hochrisikosysteme)

Soweit Art. 5 Abs. 1 lit. h bzw. lit. e Fernidentifizierungssysteme nicht bereits verbietet, greifen die Anforderungen an Hochrisiko-KI-Systeme aus Art. 6 Abs. 2 i. V. m. Anhang III Nr. 1 lit. a KI-VO für den nachträglichen biometrischen Abgleich einer Person mit einer Referenzdatenbank. Die Behörden müssen deshalb die besonderen Betreiberpflichten für Systeme zur

²¹ Art. 5 Abs. 1 lit. e KI-VO verbietet lediglich das Scraping nach Gesichtsbildern. Andere biometrische Daten, wie bspw. Stimmen, erfasst das Verbot nicht.

²² Zur rechtlichen Zulässigkeit von Clearview siehe *Martini/Kemper*, CR 2023, 414 ff.

²³ Dazu *Lewandowski*, Braucht die Polizei eine Datenbank zum biometrischen Abgleich? 2025, S. 15 ff.

nachträglichen biometrischen Identifizierung aus Art. 26 Abs. 10 KI-VO einhalten. Insbesondere muss das Gesetz sicherstellen, dass Sicherheitsbehörden²⁴ keine Entscheidungen treffen, die *ausschließlich* auf Grundlage des automatisiert generierten Ergebnisses beruhen. Dies macht eine Regelung erforderlich, die wirksam unterbindet, dass vermeintliche Treffer aus den eingesetzten Systemen automatisch Ermittlungsmaßnahmen auslösen. Eine solche in den Gesetzentwurf aufzunehmen, empfiehlt sich jedenfalls aus Klarstellungsgründen.

B. Fachfragen zu einzelnen Normen

I. Zu § 11

Frage 20

Welche materiellen Anforderungen ergeben sich aus Ihrer Sicht daraus, dass der Entwurf explizit auch die Versammlungsfreiheit als einschränkbares Grundrecht benennt? Handelt es sich nach Ihrem Dafürhalten um eine bloße formelle Zitierregelung oder sehen Sie das Risiko, dass der erweiterte in der Praxis als Blanko-Legitimation umfassend für Vorfeld- und Überwachungsmaßnahmen dienen könnte? Wie begründen Sie Ihre Auffassung?

Die Versammlungsfreiheit ausdrücklich als eingeschränktes Recht zu benennen, entspricht den Vorgaben des verfassungsrechtlichen Zitiergebots (Art. 19 Abs. 1 S. 2 GG): Die Legislative muss offenlegen, in welche Grundrechte ein Gesetz typischerweise eingreifen darf.

Das Zitiergebot soll den Gesetzgeber dazu anhalten, sich die Reichweite und Intensität möglicher Grundrechtseingriffe vor Augen zu führen und diese kritisch zu reflektieren. Es erschöpft sich nicht in einer bloßen formellen Regelung.

Die Normänderung erweitert aber die bestehenden Befugnisse der Polizei nicht in greifbarer Weise, sondern macht transparent und stellt klar, dass einzelne polizeiliche Maßnahmen auch versammlungsrelevante Implikationen haben. Das gilt etwa für polizeiliche Maßnahmen im Vorfeld einer Versammlung oder nach deren Auflösung sowie für Maßnahmen bei nicht-öffentlichen Versammlungen, für die das Versammlungsgesetz grundsätzlich nicht gilt.

²⁴ Zu den Normadressaten gehören nicht nur Strafverfolgungs-, sondern auch Gefahrenabwehrbehörden; vgl. Art. 2 Nr. 45 lit. a KI-VO.

Auch andere Landesgesetzgeber (wie NRW mit § 7 PolG NRW seit 2019) haben die Versammlungsfreiheit ausdrücklich in ihre Zitierregelung aufgenommen. Die Gesetzgeber unterstreichen damit ein gewachsenes Problembewusstsein hinsichtlich versamlungsbezogener Maßnahmen und der verfassungsrechtlichen Bedeutung des Zitiergebots.

Die Änderung birgt aber zugleich keine Blanko-Legitimation für polizeiliches Handeln. Insbesondere ändert sie (jedenfalls bei sachgerechter Interpretation) an dem Grundsatz der Polizeifestigkeit des Versamlungsrechts nichts. Dieser ergibt sich aus dem systematischen Verhältnis der Normkomplexe zueinander und den damit verbundenen verfassungsrechtlichen Implikationen. Die Polizeifestigkeit des Versamlungsrechts hindert es nicht, für nicht versamlungsspezifische Gefahren das Polizeigesetz anzuwenden. Die Versamlungsfreiheit kann mit anderen Worten nicht ausschließlich durch das Versamlungsgesetz beschränkt werden.²⁵ Soweit das Versamlungsgesetz Rechtslücken aufweist, darf ergänzend (in den Grenzen des Gebots der Polizeifestigkeit des Versamlungsrechts) auf das allgemeine Polizeirecht zurückgegriffen werden.

II. Zu § 21

1. 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 Zwangsmaßnahmen?

Ausweislich der Gesetzesbegründung soll die Videoüberwachung in Gewahrsamseinrichtungen vorrangig die in Gewahrsam genommene Person schützen (Art. 2 Abs. 2 S. 1 GG), daneben dient sie auch dem Schutz von Polizeibediensteten. Der neu einzufügende § 21 Abs. 4 PAG-E knüpft an eine erhöhte abstrakte Gefahr an, die den Schutz

²⁵ Vgl. etwa BVerwG, Urt. v. 27.3.2024, Az. 6 C 1.22 = BVerwG NVwZ 2024, 1008 Rn. 34.

von Personen gebietet. Dem steht das allgemeine Persönlichkeitsrecht des Betroffenen (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) gegenüber. Mit dem Eingriff verknüpft sich ein erheblicher Eingriff in Grundrechte. Für Hafträume hat das Bundesverfassungsgericht bereits festgestellt, dass die Videoüberwachung hohen grundrechtlichen Hürden unterworfen ist.²⁶

Eine Überwachung kann die ohnehin bestehende Anspannungssituation des Betroffenen zusätzlich verstärken. Insbesondere erzeugt die ständige Beobachtung einen psychischen Anpassungsdruck, welcher nachhaltige Einschüchterungseffekte nach sich ziehen kann. Diese Eingebundenheit erzeugt bereits für sich genommen eine erhebliche psychische Vulnerabilität und verstärkt das Gefühl, staatlicher Hoheitsmacht ausgeliefert zu sein. Der Betroffene kann der Überwachung auch nahezu nicht ausweichen. Sobald keine erhebliche Gefahr einer Selbst- oder Fremdverletzung mehr droht oder sie in die Intimsphäre des Betroffenen eingreift, ist sie jedenfalls nicht mehr mit dem allgemeinen Persönlichkeitsrecht vereinbar.

Der Gesetzesentwurf stellt zwar ausdrücklich klar, dass der Schutz der Intimsphäre zu wahren ist (S. 2). Wie das aber genau erfolgen soll, bleibt unklar. Es ist mindestens empfehlenswert, normativ klarzustellen, durch welche Schutzmechanismen tatsächlich die Wahrung der Intimsphäre sichergestellt ist.

Für in Gewahrsam genommene Personen trifft den Staat eine besondere Schutzpflicht. Das gilt vor allem dann, wenn deren Zustand auf eine erhebliche Gefahr für Leib oder Leben schließen lässt. In einem solchen Fall ist sicherzustellen, dass die Gefahrprognose tatsächlich begründet ist und zur Verfügung stehende, weniger eingriffsintensive Maßnahmen (z. B. kontaktlose Überwachung von Vitalzeichen) vorrangig zu ergreifen sind, soweit diese hinreichend wirksam sind. Eine Videoüberwachung während der Ingewahrsamnahme ist daher nicht per se unangemessen, bedarf aber einer strengen einzelfallbezogenen Rechtfertigungsprüfung.

2. Frage 32

Welche gesetzlichen Änderungen empfehlen Sie, damit Gewahrsamsüberwachung nicht zur Normalität wird? Sollte aus Ihrer Sicht – ähnlich wie im bereits geltenden § 33a PAG

²⁶ BVerfG, NSTZ 1999, 428 (429); BVerfG NJW 2015, 2100 (2101).

(Bodycam) – auch das polizeiliche Gegenüber die Möglichkeit erhalten, eine Aufzeichnung der Gewahrsamsräume zu verlangen?

Berichte über mutmaßliche Polizeigewalt bei Personen, die sich in staatlicher Obhut befinden, häufen sich. Auch vor diesem Hintergrund will der Gesetzesentwurf die Überwachungsmaßnahmen als Schutz der in Gewahrsam befindlichen Person – und damit als Instrument des Grundrechtsschutzes der Gewahrsamsperson sowie als Transparenzmechanismus zur gegenseitigen Absicherung – verstanden wissen. Dies legt mit Blick auf die besondere psychische Belastungssituation einen greifbaren Schutzmechanismus nahe, der sowohl Polizeibedienstete als auch in Gewahrsam genommene Personen vor Übergriffen, sich zuspitzenden Eskalationen und unbegründeten Vorwürfen schützt. Es ist daher konsequent, der betroffenen Person ein Recht einzuräumen, auf Verlangen eine Aufzeichnung zu erhalten. Die geforderte Überwachung kann zur nachvollziehbaren Aufklärung des Geschehens beitragen und das Vertrauen in die Polizeiarbeit stärken. Da es sich bei der Gewahrsamsüberwachung um einen erheblichen Grundrechtseingriff handelt, ist es auch angezeigt, dass der Gesetzgeber eine zeitliche Begrenzung der Überwachung sowie ggf. eine richterliche Bestätigung bei länger andauernder oder besonders eingriffsintensiver Überwachung vorsieht.

III. Zu § 33

Frage 42

Welche verfassungsrechtlichen Risiken sehen Sie in der Kombination aus „Videoüberwachung, automatischer Verhaltensanalyse und automatisierter Nachverfolgung“, insbesondere hinsichtlich der Normenklarheit „Verhaltensmuster“, der Versammlungsfreiheit und sogenannter „Chilling Effects“?

Die Kombination aus (dauerhafter) Videoüberwachung, algorithmischer Verhaltensanalyse und automatisierter Nachverfolgung, die im Vorfeld von Versammlungen, bei Ansammlungen oder sonstigen öffentlichen Veranstaltungen greift, kann einschüchternd wirken und Menschen davon abhalten, an Veranstaltungen teilzunehmen. Solche „chilling effects“ beeinträchtigen die freie Ausübung der Versammlungsfreiheit bereits im Vorfeld staatlicher Maßnahmen. Wenn Teilnehmende befürchten müssen, ihr Verhalten werde automatisiert analysiert, gespeichert und nachverfolgt, kann dies die offene, politische Meinungsbildung erheblich beeinträchtigen.

Automatisierte Systeme erfassen typischerweise nicht nur konkrete Gefährder, sondern verarbeiten zwangsläufig auch Daten unbeteiligter Personen. Das widerspricht grundsätzlich dem Gebot, Überwachungsmaßnahmen gezielt auf Personen zu beschränken, die als potenzielle Verursacher von erheblichen Gefahren in Betracht kommen.

§ 33 Abs. 4 PAG-E birgt deshalb erhebliche verfassungsrechtliche Risiken. Besonders herausfordernd sind die mangelnde Normenklarheit des Begriffs „Verhaltensmuster“, mögliche Eingriffe im Vorfeld von Versammlungen sowie Abschreckungseffekte („chilling effects“) auf die Wahrnehmung anderer demokratischer Freiheitsrechte.²⁷

Das Gebot der Normenklarheit verlangt, dass Betroffene vorhersehen können, unter welchen Voraussetzungen der Staat personenbezogene Daten erhebt und verarbeitet. Der Gesetzgeber muss deshalb die Gründe und Kriterien für eine automatisierte Überwachung hinreichend bestimmt festlegen. § 33 Abs. 4 PAG-E konkretisiert diese Vorgabe, indem die Norm festlegt, dass *„[d]ie automatische Auswertung [...] nur auf das Erkennen solcher Verhaltensmuster ausgerichtet sein [darf], die auf die Entstehung einer Gefahrensituation oder die Begehung einer Straftat hindeuten.“*

Der Begriff „Verhaltensmuster“ bleibt jedoch unbestimmt. In der Rechtssoziologie beschreiben „Verhaltensmuster“ allgemein typische Regelmäßigkeiten sozialen Verhaltens. Die Norm legt aber nicht fest, welche konkreten Verhaltensweisen eine automatisierte Analyse auslösen dürfen. Für Betroffene bleibt damit unklar, welches Verhalten sie in den Fokus polizeilicher Beobachtung rücken lässt. Die Vorschrift eröffnet der Polizei und den eingesetzten Systemen daher einen erheblichen Interpretations- und Entscheidungsspielraum. Gerade bei automatisierten Verfahren steigt damit das Risiko einer anlasslosen und übermäßigen Überwachung auch unbeteiligter Personen.

Nimmt man den Wortlaut der Vorschrift ernst („auf die Entstehung einer Gefahrensituation oder die Begehung einer Straftat hindeuten“), genügt jede sich andeutende Gefahrensituation, um eine Auswertung zu rechtfertigen. Das schließt über das Ziel hinaus. Denn es gestattet eine generelle Auswertung bei jedem Hinweis auf eine irgendwie geartete Gefahrenlage. Der

²⁷ Zu Einschüchterungseffekten visueller Polizeiüberwachung bei Versammlungen siehe bspw. *Martini/Thiessen et al.* (Fn. 2), S. 53 f.

Gesetzgeber sollte die Art und Schwere der Gefahrenlage konkretisieren. Es empfiehlt sich, Videoüberwachungen und automatisierte Analysen auf solche Konstellationen zu beschränken, in denen tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass von einer Veranstaltung *erhebliche* (idealerweise näher konkretisierte) Gefahren für die öffentliche Sicherheit oder Ordnung ausgehen. Nach jetzigem Stand des Entwurfs rechtfertigt auch *jede Straftat* eine Auswertung. Der Gesetzgeber sollte diese grundrechtsintensive Maßnahme spezifischen Straftaten bzw. Straftaten bestimmter Schwere vorbehalten.

IV. 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?

Der Einsatz von Drohnen ergänzt bereits seit einigen Jahren das technische Instrumentarium von Sicherheitsbehörden. Es erfährt zudem wachsende Bedeutung.²⁸ So sehr diese Technologie die polizeiliche Arbeit nachhaltig zu vereinfachen und zu unterstützen vermag, schwebt über ihr zugleich das Damoklesschwert eines psychosozialen Bedrohungspotenzials für die Bevölkerung sowie einer zunehmenden staatlichen Überwachungsichte.

a) Technische Spezifika von Drohnen

Drohnenaufnahmen in Gestalt einer reinen Live-Videobeobachtung (sog. Kamera-Monitor-Prinzip) sind weniger grundrechtssensibel als eine Speicherung von Aufnahmen. Das Geschehen lässt sich in einem solchen Fall nur in Echtzeit verfolgen, solange die Drohne fliegt; die Bildübertragung ist ohnedies erforderlich, um das Gerät steuern zu können. Bereits diese Form der Beobachtung kann jedoch durch moderne Fokussierungsfunktionen Personen individualisieren und erhebt zumindest kurzzeitig personenbezogene Daten. Sie greift damit in das Recht auf informationelle Selbstbestimmung ein.

²⁸ Siehe hierzu auch *Martini*, DÖV 2019, 732 f.

Sobald die Aufnahmen gespeichert und nachträglich ausgewertet werden können, steigt die Grundrechtsintensität des Eingriffs erheblich. Die Aufzeichnung von Videodaten eröffnet die Möglichkeit, die Daten später auszuwerten. Die Fortschritte der Informationstechnologie machen es möglich, selbst größere Übersichtsaufnahmen mit niedriger Auflösung nachträglich zu bearbeiten und dabei einzelne Personen oder zumindest identifizierungsrelevante Merkmale sichtbar zu machen.

Hinzu kommt die besondere technische Eigenart von Drohnen. Bei Flugdrohnen, die mit moderner Überwachungstechnik ausgestattet sind, handelt es sich nicht lediglich um ein gleichsam technisch optimiertes Auge wie bei einem herkömmlichen Fernglas. Die Luftperspektive eröffnet den Sicherheitsbehörden vielmehr ein deutlich breiteres und übersichtlicheres Lagebild, das früher nur durch den Einsatz von Hubschraubern o. ä. möglich war.

Drohnen können sich zudem dem Wahrnehmungsbereich der Betroffenen weitgehend entziehen, sobald sie eine gewisse Flughöhe erreicht haben. Gleiches gilt für die akustische Wahrnehmung. Damit unterscheiden sie sich auch von herkömmlicher Überwachungstechnik, die in der Regel deutlich auffälliger platziert und damit auch leichter erkennbar ist. Im Gegensatz zu fest installierten Überwachungskameras sind moderne Drohnen auch Ausdruck „verflüchtigter“ Überwachung, weil sie grundsätzlich flexibel und ortsunabhängig einsetzbar sind.²⁹ Auch Hinweisschilder ändern daran wenig, da diese bei größeren Menschenansammlungen leicht übersehen werden können. Zugleich können sich die Betroffenen der Aufnahme aus der Vogelperspektive nur eingeschränkt entziehen.

Aus all diesen Umständen erwachsen ein erheblicher Überwachungsdruck sowie Einschüchterungseffekte. Die vom Boden aus beobachteten Personen können auch regelmäßig nicht verlässlich einschätzen, ob lediglich eine Echtzeitbeobachtung stattfindet oder ob die Polizei die Aufnahmen auch speichert und auswertet. Dies kann dazu führen, dass Betroffene künftig davon Abstand nehmen, ihre Freiheitsrechte auszuüben.

Der polizeiliche Drohneneinsatz zeichnet sich nicht zuletzt durch eine erhebliche Streubreite aus. Wenn eine Drohne eine Menschenmenge überfliegt, erfasst sie vielfach auch Unbeteiligte,

²⁹ Siehe zum Ganzen *Martini* (Fn. 28), 736.

die sich nicht auf die konkrete Beobachtung einstellen können.³⁰ Gerade diese Personen sind einem diffusen Gefühl ständiger Überwachung ausgesetzt, obgleich sie ggf. lediglich von ihren grundrechtlich geschützten Freiheiten Gebrauch machen wollen.

b) Rechtliche Schlussfolgerungen

Das Eingriffsniveau einer Drohne bestimmt sich außer aus der Streubreite der Maßnahme, dem Ausmaß von Auswirkungen auf Nichtstörer sowie der Intensität der Datenverarbeitung maßgeblich nach der technischen Ausgestaltung der Aufnahme sowie nach der weiteren Verwendung der Daten.

Je intensiver die Drohnenüberwachung in die informationelle Selbstbestimmung eingreift, desto bestimmter muss die polizeiliche Ermächtigungsgrundlage sein. Das ergibt sich aus dem verfassungsrechtlichen Gebot der Normenklarheit und Bestimmtheit: Der Gesetzgeber muss den Drohneneinsatz so hinreichend klar bestimmen, dass der Einsatz im Hinblick auf Anlass, Zweck und Ausmaß vorhersehbar ist und der Bürger sich auf den damit einhergehenden Grundrechtseingriff sachgerecht einstellen kann.

Auch die konkrete Flughöhe und technische Ausgestaltung der Überwachungstechnik sind für die grundrechtliche Eingriffsintensität relevant: Findet die Videoüberwachung bspw. in einer Höhe statt, in der Menschen zwar anhand ihrer Umrisse als solche erkennbar sind, die individuelle Person aber nicht identifizierbar ist, liegt kein Eingriff vor;³¹ anders jedoch, wenn die technische Ausgestaltung des Objekts mittels Fokussierungsmitteln auch aus weiter Höhe eine Identifizierung möglich macht.

Nimmt das Zusammentreffen der Menschen die Qualität einer durch Art. 8 Abs. 1 GG geschützten Versammlung an, ist nicht das PAG, sondern das Versammlungsgesetz einschlägig. In diesem Falle kann sich die Sicherheitsbehörde wegen der Polizeifestigkeit des Versammlungsrechts nicht auf § 38 PAG-E berufen. Auch ein Rückgriff auf §§ 12a, 19a VersG scheidet aus, da Drohnen nicht den bestimmtheitsrechtlichen Anforderungen bekannter Mittel der Bild- und Tonaufnahme entsprechen.³² Besonders die versammlungsspezifische

³⁰ Martini/Thiessen et al. (Fn. 2), S. 92.

³¹ Martini (Fn. 28), 735.

³² Martini/Thiessen et al. (Fn. 2), S. 93 f.

Eingriffswirkung, die von Drohnen ausgeht, verlangt aus verfassungsrechtlicher Sicht eine eigene Rechtsgrundlage für den Drohneneinsatz.³³

V. Zu § 43a

1. Frage 106

Gehen mit dem neuen § 43a aus Ihrer Sicht grund- und menschenrechtliche Risiken einher, mit Blick auf biometrische Massenbetroffenheit, Fehlzusammenordnungen, Diskriminierung und sogenannte Chilling Effects?

Der nachträgliche automatisierte biometrische Abgleich mit öffentlich frei zugänglichen personenbezogenen Daten aus dem Internet berührt eine Vielzahl grund- und menschenrechtlicher Schutzpositionen, die sowohl auf internationaler, europäischer sowie auf bundes- und landesverfassungsrechtlicher Ebene verankert sind. Er greift – insbesondere mit Blick auf die Breite der Datenerfassung und die hohe Streuwirkung gegenüber unbeteiligten Dritten – tief in das Recht auf informationelle Selbstbestimmung bzw. den Schutz personenbezogener Daten ein und kann aufgrund nicht auszuschließender Verzerrungen und Fehlzusammenordnungen zugleich mit der Gewährleistung des Art. 3 Abs. 3 GG, Art. 14 EMRK bzw. Art. 21 Abs. 1 GRCh konfliktieren. Das Bundesverfassungsgericht betonte in der Vergangenheit bereits, dass die Verknüpfung der Analyse- oder Auswertungseinrichtung mit dem Internet eine besonders eingriffsverstärkende Wirkung entfaltet.³⁴

Solche Eingriffe können darüber hinaus zu einem Gefühl des ständigen Überwachtseins und infolgedessen zu einer Einschüchterung der Grundrechtsträger führen. Gleichzeitig lösen heimliche Massenüberwachungsmaßnahmen systemische Freiheitsstörungen aus, die über die abwehrrechtliche Grundrechtsfunktion hinausgehen.³⁵

Das Training der zum automatisierten Abgleich eingesetzten KI-Systeme erfolgt auf Grundlage historischer Daten, in denen sich bestehende gesellschaftliche und institutionelle Muster

³³ Martini/Thiessen et al. (Fn. 2), S. 93; zum „Wie“ der verfassungsrechtlichen Ausgestaltung bei Versammlungen Martini (Fn. 28), 740 f.

³⁴ BVerfGE 165, 383 (404).

³⁵ Gärditz, in: Stern/Sodan/Möstl, Das Staatsrecht der Bundesrepublik Deutschland im europäischen Staatenverbund, 2. Aufl. 2022, § 22 Innere Sicherheit Rn. 67.

widerspiegeln. Solche Daten weisen oftmals Verzerrungen (Biases) auf, die bspw. bei Menschen mit asiatischem Aussehen oder Schwarzen zu einer deutlich höheren Fehlerrate führen.³⁶ Der Einsatz solcher Systeme birgt daher die Gefahr, bereits bestehende gesellschaftliche Diskriminierungsstrukturen zu reproduzieren und zu verfestigen.³⁷ Gleichzeitig bleiben Entscheidungsfindungsprozesse algorithmenbasierter Systeme selbst für Entwickler häufig intransparent (sog. Black-Box-Phänomen),³⁸ sodass diskriminierende Wirkungen im Einzelnen oftmals unentdeckt bleiben. Fehlerhafte Zuordnungen können darüber hinaus unbeteiligte Personen in den Fokus polizeilicher Ermittlungsarbeit rücken und verstärken damit zusätzlich die Eingriffsintensität. Maßnahmen mit einer derart hohen Eingriffsintensität dürfen nur bei hinreichend konkretisierten Gefahren für besonders wichtige Rechtsgüter stattfinden.³⁹

2. Frage 112

Wie bewerten Sie den Richtervorbehalt in § 43a?

Der Richtervorbehalt nach § 43a Abs. 2 PAG-E reagiert auf die zwingende Vorgabe des Art. 26 Abs. 10 KI-VO.⁴⁰ Dem liegt eine sachgerechte rechtspolitische Erwägung zugrunde: Da der nachträgliche biometrische Datenabgleich tief in das allgemeine Persönlichkeitsrecht der Betroffenen eingreift, sollte – unabhängig von der Notwendigkeit der Maßnahme im Einzelfall – eine neutrale und unabhängige Instanz über den Einsatz entscheiden. Gerade bei derart eingriffsintensiven KI-gestützten Überwachungsmethoden ist gesellschaftliches Vertrauen von essenzieller Bedeutung.

³⁶ Grother/Ngan/Hanaoka (NIST), Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, Dezember 2019, S. 2; Buolamwini/Gebbru, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, Proceedings of Machine Learning Research 81, 2018, 1-15; Angwin/Larson/Mattu/Kirchner, ProPublica, Machine Bias, Online-Artikel v. 23.05.2016, <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>.

³⁷ Martini, Blackbox Algorithmus, 2019, S. 44 ff.; Ogorek, LTZ 2024, 274 (280).

³⁸ Vgl. Martini, Blackbox Algorithmus, 2019, S. 41 ff.; Martini/Botta, „Sehende Steine“ statt „Kommissar Zufall“? – Künstliche Intelligenz im Dienste der Polizei, DÖV Blog v. 23.2.2026, „Sehende Steine“ statt „Kommissar Zufall“? – Künstliche Intelligenz im Dienste der Polizei | DÖV Blog, zum allgemeinen Einsatz von KI in der Polizeiarbeit.

³⁹ BVerfG 165, 363 (364); Martini/Botta, „Sehende Steine“ statt „Kommissar Zufall“? – Künstliche Intelligenz im Dienste der Polizei, DÖV Blog v. 23.02.2026, „Sehende Steine“ statt „Kommissar Zufall“? – Künstliche Intelligenz im Dienste der Polizei | DÖV Blog mit korrespondierender Kritik an bereits existierenden landesrechtlichen Regelungen zur automatisierten Datenanalyse.

⁴⁰ Die Erläuterungen des Gesetzentwurfs zu Nummer 34 (Einfügung des § 43a) verweisen im Zusammenhang mit dem Richtervorbehalt zu Absatz 2 fälschlicherweise auf Art. 24 Abs. 10 KI-VO (S. 54). Diese Norm existiert nicht. Gemeint ist Art. 26 Abs. 10 KI-VO.

3. Frage 113

Welche Anforderungen an den nachträglichen biometrischen Abgleich mit öffentlich frei zugänglichen Internetdaten (§ 43a) ergeben sich aus der Verordnung über künstliche Intelligenz der EU?

Siehe dazu die Antwort zu Frage 16 unter 2. lit. b, S. 9.

Landtag Kordilewski, Astrid

Von: Martini, Mario <mario.martini@unibw.de>
Gesendet: Dienstag, 2. Juni 2026 22:23
An: Landtag Poststelle
Cc: anna.berry@foev-speyer.de; Schuchort, Tom; Haspinger, Luci
Betreff: PAG Thüringen
Anlagen: Martini PAG Thüringen.pdf
Signiert von: mario.martini@unibw.de

Sehr geehrter Herr Dr. König,
sehr geehrter Herr Dr. Hyckel,
sehr geehrter Herr Linse,
sehr geehrte Damen und Herren,

nunmehr konnte ich meine Stellungnahme abschließen und füge diese ihnen in der Anlage bei. Nochmals herzlichen Dank für die gewährte Fristverlängerung. Ich bin mit der Veröffentlichung der Stellungnahme einverstanden. Für Rückfragen stehe ich Ihnen selbstverständlich sehr gerne zur Verfügung.

Mit den besten Grüßen
Mario Martini