

Den Mitgliedern des
AfIKL

Prof. Dr. iur. Kristin Pfeffer

THUR. LANDTAG POST
26.05.2026 06:43

15803 | 2026

FORSCHUNGSSTELLE EUROPÄISCHES UND DEUTSCHES SICHERHEITSRECHT (FEDS)

Prof. Dr. iur. Kristin Pfeffer, Hochschule der Polizei Hamburg, Überseering 35, 22297 Hamburg

An den Thüringer Landtag
Ausschuss für Inneres, Kommunales und Landesentwicklung
Jürgen-Fuchs-Straße 1

99096 Erfurt

Thüringer Landtag
Z u s c h r i f t
8/563

zu Drs. 8/2478



Akademie
POLIZEI

Hochschule der Polizei Hamburg
University of Applied Sciences
Überseering 35
D-22297 Hamburg

E-Mail: kristin.pfeffer@ak.polizei.hamburg.de

Vorab per Email poststelle@thueringer-landtag.de

**Zweites Gesetz zur Änderung des Polizeiaufgabengesetzes – Gesetzesentwurf der Landesregierung –
Drucksache 8/2478**

Schriftliches Anhörungsverfahren im Ausschuss für Inneres, Kommunales und Landesentwicklung

Hamburg, 24. Mai 2026

Sehr geehrte Damen und Herren Abgeordnete,

anbei darf ich Ihnen meine Stellungnahme zum o.g. Gesetzesentwurf übersenden. Ich hoffe, die aufgezeigten Punkte können Sie bei Ihrer Entscheidungsfindung unterstützen.

Mit freundlichen Grüßen

Prof. Dr. Kristin Pfeffer



Stellungnahme

Zum Entwurf des Zweiten Gesetzes zur Änderung des Polizeiaufgabengesetzes – Gesetzesentwurf der Landesregierung – Drucksache 8/2478

Zu § 40a ThürPAG-E (Fragen Nr. 93- 104)

I. Vorbemerkung

Mit ihrem Gesetzesentwurf „Zweites Gesetz zur Änderung des Polizeiaufgabengesetzes – Gesetzesentwurf der Landesregierung – Drucksache 8/2478“ schlägt die Landesregierung neue Eingriffsbefugnisse für die Polizei vor, die erkennbar von dem Anspruch geprägt sind,

- die Effektivität der Gefahrenabwehr zu erhöhen,
- insbesondere auf die rasante Fortentwicklung der Datafizierung der Polizeiarbeit zu reagieren,
- die Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 (KI-VO),
- die zwischenzeitlich ergangen Entscheidungen des BVerfG umzusetzen.

Die nachfolgende Stellungnahme beschränkt sich auf einige Anmerkungen zu den Fragen (Nr. 93-104) zum Regelungsvorschlag des § 40a ThürPAG-E (Anlassbezogene automatisierte Datenanalyse)

Diese betreffende Befugnis ist äußerst eingriffsintensiv. Neben den Vorgaben des BVerfG (Urteil vom 16. Februar 2023 - 1 BvR 1547/19 zu den Eingriffsbefugnissen von Hamburg und Hessen) sind hier (soweit nicht die nationale Sicherheit iSv Art. 4 EUV betroffen ist) auch die europarechtlichen Vorgaben zu beachten. Das mitgliedstaatliche Polizeirecht ist in diesen Bereichen durch die DSRL-JI und die KI-VO (teilweise) harmonisiert worden. Wie sich aus den nachfolgenden Ausführungen ergibt, verstoßen die hier näher betrachteten Regelungsvorschläge derzeit in einigen Punkten gegen Verfassungsrecht. Sie wären in diesen Punkten vor ihrer Verabschiedung noch anzupassen.

II. Prüfungsmaßstab

Trotz der Feststellung einer „verfassungsfesten Integrationsschranke“ durch das Lissabon-Urteil des BVerfG und trotz der Verankerung des Ordre-public-Vorbehalts im Primärrecht der EU unterliegt das Recht im Bereich des Raumes der Freiheit der Sicherheit und des Rechts seit dem Vertrag von Lissabon einer zunehmenden Europäisierung.¹ Während das Recht der EU/EG zunächst primär auf Polizeikooperation ausgerichtet war, hat sich in den letzten Jahren ein Paradigmenwechsel vollzogen hin zu einer Harmonisierung des Sicherheitsrechts.² In den harmonisierten Bereichen des Sicherheitsrechts hat diese Entwicklung weitreichende Folgen für die Geltung der Unionsgrundrechte, wobei zwischen teil- und vollharmonisierten Bereichen zu unterscheiden ist:

¹ So bereits von Arnauld, JA 2008, S. 327 ff.

² von Arnauld, JA 2008, S. 327 ff.; Hecker, DÖV 2006, 273ff.

Für den Bereich des vollharmonisierten mitgliedstaatlichen Rechts, wie etwa in Teilbereichen des Datenschutzrechts der DS-GVO, hat sich das BVerfG im Jahr 2019 mit seiner Entscheidung „Recht auf Vergessen II“ bereits neu positioniert³: Bei der Anwendung unionsrechtlich vollständig vereinheitlichter Regelungen sind nunmehr nach dem Grundsatz des Anwendungsvorrangs des Unionsrechts in aller Regel nicht die Grundrechte des Grundgesetzes, sondern allein die Unionsgrundrechte maßgeblich. Das BVerfG greift deshalb bei der grundrechtlichen Überprüfung der Rechtsanwendung durch die deutsche Gewalt im Bereich DS-GVO auf die Grundrechte-Charta zurück.⁴ Andere mitgliedstaatliche Verfassungsgerichte verfahren bereits so.⁵ Unionsgrundrechte erfassen hier also einen besonders sensiblen Regelungsbereich, insbesondere mitgliedstaatliches Polizeirecht, d.h. gerade den Bereich, der regelmäßig als Prüfstein der Rechtsstaatlichkeit, insbesondere des Grundrechtsschutzes eines Mitgliedstaates gilt.⁶ Kritiker sehen in der „Letztauslegung“ durch den EuGH eine Aushöhlung des nationalen, ebenfalls „von der nationalen Kultur geprägten Grundrechtsschutzes“⁷.

Die durch die Umsetzung von Sekundärrecht geschaffenen mitgliedstaatlichen Normen und die hierauf beruhenden Maßnahmen der Mitgliedstaaten sind – zumindest teilweise – auch an den Unionsgrundrechten zu messen (hier regelmäßig Teilharmonisierung). Der EuGH legt hier die grundrechtlichen Schutzgehalte fest.⁸

Der Harmonisierungsgrad des mitgliedstaatlichen Sicherheitsrechts durch die KI-VO lässt sich allerdings nicht einheitlich bestimmen, er hängt von der jeweiligen konkreten Bestimmung der KI-VO ab.⁹ Im Bereich der sog. Hochrisiko-KI-Systeme nach Art. 6 ff. KI-VO, zu denen auch die Systeme zur automatisierten Datenanalyse zur Gefahrenabwehr durch Sicherheitsbehörde zählen¹⁰ (dazu näher unter III. 2.), steht es den Mitgliedstaaten weiter offen, KI-Systeme im Bereich der Gefahrenabwehr und Strafverfolgung einzusetzen. Die Mitgliedstaaten können Ermächtigungsgrundlagen schaffen, die noch weitergehende Vorgaben enthalten, sofern diese nicht die technisch-organisatorischen Vorgaben der KI-VO betreffen,¹¹ müssen aber dabei die Vorgaben und Anforderungen, die dann nach der KI-VO für Hochrisiko-KI-Systeme gelten, zwingend beachten.

Den Mitgliedstaaten verbleibt so im Bereich des Einsatzes von Hochrisiko-KI-Systemen im Bereich Gefahrenabwehr und Strafverfolgung sowohl nach der DSRL-JI, als auch nach der KI-VO nach wie

³ BVerfGE 152, 216 = NJW 2020, 314 Rn. 1-142.

⁴ BVerfGE 152, 216 = NJW 2020, 314 Rn. 1-142 dazu Kühling, NJW 2020, S. 227 ff.

⁵ Verfassungsgerichtliche Prüfung anhand der Grundrechte-Charta durch ÖstVerfGH, Erkenntnis v. 14.03.2012 – U 466/11 ua ECLI:AT:VFGH:2012:U466.2011, sub. 5.5; BelgVerfGH Entsch. v. 15.03.2018 – 29/2018, B 9, B 10.5, B 15 ff.; Conseil Constitutionnel, Urt. v. 26.7.2018 – 2018-768 DC Rn. 10, 12, 38; Corte costituzionale, Entsch. v. 23.1.2019 – 20/2019 ECLI:IT:COST:2019:20 Rn. 2.1, 2.3.

⁶ So bereits Bäcker/Hornung, ZD 2012, S. 147, 149.

⁷ Valta/Vasel, ZRP 2021, 142 (143 f.).

⁸ So bereits Bäcker/Hornung, ZD 2012, S. 147, 149; Bäcker, in: Hill/Kugelman/Martini (Hrsg.) Perspektiven der digitalen Lebenswelten 2017, S. 63 (84 ff.).

⁹ Hofmann-Coombe, EuR 2025, 363, 377 unter Verweis auf BVerfGE 152, 216, 247.

¹⁰ Schöndorf-Haubold/Giogios, KI im Einsatz für die Sicherheit: Innovation und Kontrolle im Spannungsfeld von europäischer Gesetzgebung und nationaler Souveränität, VerBlog, 2024/12/10, <https://verfassungsblog.de/ki-im-einsatz-fur-die-sicherheit/> (Zugriff: 09.02.2026).

¹¹ Guckelberger, DÖV 2025, 45, 45f.; Hofmann-Coombe, EuR 2025, 363, 379.

vor ein substanzieller Spielraum (Teilharmonisierung), so dass hier der Prüfungsmaßstab das Grundgesetz bleibt und nicht die Charta der Grundrechte.¹² Daneben sind der Vorgaben aus der DSRL-JI und der KI-VO zu beachten (hierzu im Einzelnen unter III.).

III. Europarechtliche Anforderungen

1. RL (EU) 2016/680 (DSRL-JI)

Die innerstaatliche polizeiliche Datenverarbeitung wurde durch die RL (EU) 2016/680 (DSRL-JI) teilharmonisiert, weshalb bei der automatisierten Datenanalyse auch die europarechtlich vorgegebenen Anforderungen zu beachten sind.¹³ Die Umsetzung erfolgt(e) in den jeweiligen Fachgesetzen des Landes- und Bundesrechts.

Im Kontext von automatisierter Datenanalyse ergibt sich aus der DSRL-JI ausdrücklich ein Verbot eines sog. Profilings (Art. 3 Nr. 4 DSRL-JI), da natürliche Personen auf der Grundlage besonderer Datenkategorien im Sinne des Art. 10 DSRL-JI (z.B. ethnische Herkunft, religiöse Überzeugungen oder sexuelle Orientierung) diskriminiert (Art. 11 Abs. 3 DSRL-JI). Solche Daten dürfen in eine polizeiliche Datenanalyse zum Zwecke des Profilings nur einfließen, wenn es dafür einen besonderen rechtfertigenden Grund gibt.

Die DSRL-JI fordert eine Datenschutzfolgeabschätzung (Art. 27 DSRL-JI), die die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung sowie die Eintrittswahrscheinlichkeit und die Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen berücksichtigt (Art. 27 Abs. 2 DSRL-JI). Sodann sind geeignete technische und organisatorische Maßnahmen zu treffen, um bei der Verarbeitung personenbezogener Daten ein dem Risiko angemessenes Schutzniveau zu gewährleisten, insbesondere im Hinblick auf die Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 29 DSRL-JI). Außerdem sind die Rechte der Betroffenen (Art. 12 ff. DSRL-JI) zu regeln, sowie eine Protokollierung (Art. 25 DSRL-JI). Insbesondere besteht die Pflicht der Behörden, über die (mögliche) Datenverarbeitung mittels automatisierter Analyse zu informieren (Art. 13 DSRL-JI). Diese Anforderungen wurde im allgemeinen Datenschutzrecht von Bund und Ländern bereits umgesetzt. Einer Umsetzung der Anforderungen der DSRL-JI in spezifischen Ermächtigungsgrundlagen für die automatisierte Datenanalyse ist daher nicht erforderlich.¹⁴

¹² Ebenso Hofmann-Coombe, EuR 2025, 363, 379; Martini/Botta DÖV 2025, 1033, 1040.

¹³ Zur Europäisierung des Polizeirechts und deren Auswirkung auf den Grundrechtsschutz insgesamt Pfeffer, NVwZ 2022, 294 ff.

¹⁴ Martini/Botta, DÖV 2025, S. 1033, 1035.

2. VO (EU) 2024/1689 (KI-VO)

Weitere Vorgaben für die automatisierte Datenanalyse im Bereich Gefahrenabwehr und Strafverfolgung folgen inzwischen auch aus der Verordnung zur Harmonisierung der mitgliedstaatlichen Gesetze im Bereich des Einsatzes künstlicher Intelligenz, der VO (EU) 2024/1689 (KI-VO).¹⁵ Die KI-VO verfolgt (erstmalig) einen sektorenübergreifenden Regelungsansatz, der die charakteristischen Herausforderungen der Regulierung von und des Umgangs mit KI-Systemen in Angriff nimmt und deren gesamten „Lebenszyklus“ (von der Entwicklung bis zur Verwendung) erfasst. Auch Sicherheitsbehörden unterliegen damit nun künftig den Anforderungen der KI-VO.¹⁶ Die EU stützt sich hierbei auf ihre Kompetenz aus Art. 114 AEUV zur Binnenmarktregulierung und Art. 16 AEUV zum Datenschutz, ErwGr 3. Ziel des Gesetzes ist ein funktionierender Binnenmarkt durch einen einheitlichen Rechtsrahmen, insbesondere für die Entwicklung, das Inverkehrbringen, die Inbetriebnahme und die Verwendung von Systemen künstlicher Intelligenz (KI-Systeme) in der Union unter Beachtung der Werte der Union, Förderung der Technologie unter gleichzeitiger Beachtung der Grundrechte, Art. 1 Abs. 1 KI-VO.

Zwischenzeitlich hat die EU-Kommission im Rahmen des sog. „Digitalen Omnibus“ für KI einen Verordnungsvorschlag zur Änderung der KI-VO vorgelegt, in welchem sie vorschlägt, die Anforderungen in der derzeit geltenden KI-VO im Bereich Hochrisiko-KI wieder abzuschwächen.¹⁷ Am 7. Mai 2026 haben sich Rat und Europäisches Parlament bereits politisch hierauf geeinigt.¹⁸

Mit dem Digitalen Omnibus zu KI sollen insbesondere die Fristen für die Geltung verschiedener Vorschriften in der KI-VO nach hinten verschoben werden, bis die Kommission eine entsprechende Entscheidung trifft, Art. 1 Ziff. 31 Entwurf eines Digitalen Omnibus zu KI. Die Anforderungen an KI-Kompetenz sollen abgeschwächt werden. Der VO-Vorschlag betrifft Hochrisiko-KI, die bereits auf dem Markt ist: Diese sollen weitgehend von der Anwendung der KI-VO ausgenommen werden, Art. 1 Ziff. 30 Entwurf eines Digitalen Omnibus zu KI. Dies wird in der Wissenschaft z.T. heftig kritisiert. Die vorgeschlagene „Amnestie“ für Hochrisiko-KI biete Anbietern zwischenzeitlich die Möglichkeit, den europäischen Markt mit missbräuchlichen Technologien zu überschwemmen, bevor die Regeln des KI-Gesetzes vollständig in Kraft treten.¹⁹

Erste Fristen aus der KI-VO wurden bereits faktisch „verschoben“. Die EU-Kommission war ursprünglich verpflichtet, bis zum 2. Februar 2026 Leitlinien für die Hochrisiko-Einstufung zu

¹⁵ Pfeffer, NVwZ 2022, S. 294 ff.; zum Harmonisierungsgrad des Polizeirechts durch die KI-VO Hofmann-Coombe, EuR 2025, S. 363, 376 ff.

¹⁶ Dazu eingehend Pfeffer, Der Einsatz künstlicher Intelligenz in der Polizeiarbeit nach dem AI-Act – Eine rechtswissenschaftliche Perspektive, in: Honekamp, Wilfried/Kemme, Stefanie (Hrsg.), Auswirkungen von KI auf die zukünftige Polizeiarbeit 2025, S. 31ff.

¹⁷ Vorschlag für eine VO (EU) 2024/1689 und (EU) 2018/1139 im Hinblick auf die Vereinfachung der Umsetzung harmonisierter Vorschriften für künstliche Intelligenz (Digital-Omnibus-Verordnung zur KI), Erwgr. 22.

¹⁸ Rat der Europäischen Union Pressemitteilung 7. Mai 2026, <https://www.consilium.europa.eu/de/press/press-releases/2026/05/07/artificial-intelligence-council-and-parliament-agree-to-simplify-and-streamline-rules/> (Zugriff: 18.05.2026).

¹⁹ Statt vieler Bieker/Nolan, Europäische KI-FOMO: Die Europäische Kommission opfert das digitale Acquis am Altar des KI-Hypes, VerfBlog, 29.01.2026, <https://verfassungsblog.de/eu-digital-law-ai-fomo-omnibus/>, DOI: 0.59704/8ea454b6677b517f.

erstellen, Art. 6 Abs. 5 KI-VO.²⁰ Diese Frist soll im Rahmen des Entwurfes zum Digitalen Omnibus zu KI bis Dezember 2027 verschoben werden.²¹ Damit verschiebt sich auch die stufenweise Einführung der KI-VO für Hochrisiko-KI-Systeme.

Ob eine Verordnung, die auch das Inverkehrbringen, die Inbetriebnahme und die Verwendung von KI-Systemen durch Gefahrenabwehr- und Strafverfolgungsbehörden regelt, überhaupt von der Gesetzgebungskompetenz der EU umfasst ist, ist wegen der essentiellen Bedeutung des Rechts der Inneren Sicherheit für die Souveränität eines Staates²² nach wie vor umstritten.²³ Die KI-VO ist an Risiken ausgerichtet, nicht an Sektoren oder Anwendungsbereichen. Mithin werden sektorspezifische Besonderheiten etwa des Polizei- und Strafrechts nur in Ansätzen berücksichtigt. Die KI-VO unterscheidet sich grundlegend von der Regulierung vieler anderer neuer Technologien, welche sich auf bestimmte Bereiche beschränken und keine entsprechende umfassende gesellschaftliche Relevanz aufweisen. Sie ist umfassender und weist eine besondere grundrechtliche Relevanz auf.²⁴

KI-Systeme für die „nationale Sicherheit“ fallen nicht in den Anwendungsbereich der KI-VO (Art. 2 Abs. 3 UAbs. 1 KI-VO). Bereits nach dem Primärrecht verbleibt die alleinige Verantwortung für die nationale Sicherheit und Aufrechterhaltung der öffentlichen Ordnung bei den Mitgliedstaaten, Art. 4 Abs. 2 Satz 3 EUV (sog. ordre-public-Vorbehalt). Der EuGH legt den Begriff der „nationalen Sicherheit“ in ständiger Rechtsprechung eng aus. Es gehe dabei um den Schutz der wesentlichen Funktionen des Staates und der grundlegenden Interessen der Gesellschaft, um „die Verhütung und Repression von Tätigkeiten, die geeignet sind, die tragenden Strukturen eines Landes im Bereich der Verfassung, Politik oder Wirtschaft oder im sozialen Bereich in schwerwiegender Weise zu destabilisieren und insbesondere die Gesellschaft, die Bevölkerung oder den Staat als solchen unmittelbar zu bedrohen (...)“. Letzteres umfasse insbesondere die Verhütung und Repression von terroristischen Aktivitäten.²⁵ Die Bekämpfung schwerer Kriminalität wird vom EuGH dagegen (nur) unter den Begriff „innere Sicherheit“ subsumiert.²⁶

²⁰Am 19. Mai 2026 hat die EU-Kommission einen Entwurf über Leitlinien zur Einstufung von Hochrisiko-KI veröffentlicht. <https://digital-strategy.ec.europa.eu/de/library/draft-commission-guidelines-classification-high-risk-ai-systems> (Zugriff: 24.05.2026).

²¹Vorschlag für eine VO (EU) 2024/1689 und (EU) 2018/1139 im Hinblick auf die Vereinfachung der Umsetzung harmonisierter Vorschriften für künstliche Intelligenz (Digital-Omnibus-Verordnung zur KI), COM(2025) 836 final, Erwgr. 22.

²²BVerfGE 123, 267 (358) – Lissabon-Vertrag.

²³BR-Drs. 488/1/21; Kritisch Pfeffer, NVwZ 2023, S. 1286, 1289; Krönke NVwZ 2024, 529, 532; Martini, in: Hilgen-dorf/Roth-Isigkeit, Die neue Verordnung der EU zur künstlichen Intelligenz, 2023, § 4 Rn. 95 ff. Peuker ZfDR 2023, 384, 384 ff.; Schöndorf-Haubold/Giogios, KI im Einsatz für die Sicherheit: Innovation und Kontrolle im Spannungsfeld von europäischer Gesetzgebung und nationaler Souveränität, VerfBlog, 2024/12/10, <https://verfassungsblog.de/ki-im-einsatz-fur-die-sicherheit/> (Zugriff: 09.02.2026).

²⁴Die Entwicklung der Verankerung des Grundrechtsschutzes während des Gesetzgebungsprozesses der KI-VO nach-zeichnend Palmiotto, The AI Act Roller Coaster: The Evolution of Fundamental Rights Protection in the Legislative Pro-cess and the Future of the Regulation. European Journal of Risk Regulation. <https://doi.org/10.1017/err.2024.97> (Zugriff: 9.02.2026).

²⁵EuGH 21.6.2022 – C-817/19 – Ligues des droits humains.

²⁶EuGH 5.4.2022 – C-140/20 – Commissioner of An Garda Síochána. Zum Trennungsprinzip zwischen Polizei und Ge-heimdiensten Denninger, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, B. Rn. 43ff.; Zur grundsätzli-chen Aufgabentrennung von Polizei und Militär Weingärtner, in: Lisken/Denninger, Handbuch des Polizeirechts, 7.

Soweit § 40a Abs. 1 Satz 1 ThürPAG-E auf die „Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes“ abzielt, unterliegen diese Eingriffstatbestände nicht der Harmonisierung durch europäisches Sekundärrecht, wie der DSRL-JI und der KI-VO.

Im Übrigen ist das KI-Gesetz als Verordnung gem. Art. 288 AEUV in allen Teilen und in jedem Mitgliedstaat verbindlich. Im Bereich Polizei- und Strafverfolgungsbehörden sind die Regeln aber durch zahlreiche Ausnahmen regelrecht „perforiert“ worden. Hier überlässt es der Gesetzgeber im Wesentlichen den Mitgliedstaaten – unter Beachtung des von der KI-VO vorgegebenen verbindlichen Mindeststandards – den Einsatz von KI-Systemen mit Ermächtigungsgrundlagen zu erlauben und zu regulieren.

Aus deutscher Sicht zu beachten ist, dass der in der KI-VO stets verwendete Begriff der „Strafverfolgung“ europarechtlich auszulegen ist und sowohl die Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten, als auch die Gefahrenabwehr für die öffentliche Sicherheit einschließt, Art. 3 Nr. 46 KI-VO. Die in der deutschen Rechtsordnung geltende klare Differenzierung zwischen Gefahrenabwehr und Strafverfolgung,²⁷ erfolgt weder in den meisten übrigen Mitgliedstaaten noch durch die EU-Organe. Der Entwurf der Leitlinien der EU-Kommission zur Einstufung von Hochrisiko-KI enthält hierzu nähere Regelungen zur Abgrenzung von Systemen, die von nationalen Geheimdiensten eingesetzt werden.²⁸

a. Verbotene Praktiken (mit Ausnahmen)

In Art. 5 Abs. 1 KI-VO werden insgesamt acht Gruppen von KI-Praktiken für grundsätzlich unzulässig erklärt, was für Systeme zur Strafverfolgung und Gefahrenabwehr in Art. 5 Abs. 1 UAbs.1 lit h i.V.m. Abs. 2 KI-VO von vornherein durch einige weitreichende Ausnahmen abgeschwächt wird. Gemäß dem risikobasierten Ansatz der KI-VO werden diejenigen Praktiken verboten, welche ein inakzeptables hohes Risiko, insbesondere für die Grundrechte, darstellen. Hier wird bei „Praktiken“ angesetzt und nicht bei KI-Systemen. Es geht hierbei um auf KI-Systeme bezogene Tätigkeiten, nämlich das Inverkehrbringen, die Inbetriebnahme und/oder die Verwendung von KI-Systemen zu einem bestimmten Zweck.²⁹ Die EU-Kommission hat zu den verbotenen Praktiken inzwischen Leitlinien im Sinne von Art. 96 Abs. 1 lit. b der KI-VO erarbeitet.³⁰

Ausdrücklich verboten ist hier nur eine Datenanalyse mittels eines KI-Systems zur Vorhersage künftiger Straftaten auf der Grundlage von Profiling bzw. Persönlichkeitsmerkmalen, Art. 5 Abs. 1 UAbs. 1 lit. d) Hs. 1 KI-VO (personenbezogenes Predictive Policing). Erfasst ist hier nur ein Predictiv Policing, welches sich ausschließlich auf ein personenbezogenes Profi-

Aufl. 2021, I. Rn. 679ff; Zu den Konflikten bei der Auslegung des Begriffs nationale Sicherheit Pfeffer, NVwZ 2023, S. 1288.

²⁷ Dazu statt vieler Graulich, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, E. Rn. 221 ff.

²⁸ Entwurf über Leitlinien zur Einstufung von Hochrisiko-KI vom 19. Mai 2026, S. 101 f., Ziff. Abs. 344 f. <https://digital-strategy.ec.europa.eu/de/library/draft-commission-guidelines-classification-high-risk-ai-systems> (Zugriff: 24.05.2026).

²⁹ Wendehorst, in: Martini/Wendehorst (Hrsg.), KI-VO, 2024, Art. 5 Rn. 2.

³⁰ Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), 4.2.2025, C(2025) 884 final. <https://digital-strategy.ec.europa.eu/de/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act> (Zugriff 09.02.2026).

ling stützt. Unterstützt die durchgeführte Analyse mit KI lediglich die menschliche Verdachtsbewertung, ist die Maßnahme nicht verboten, Art. 5 Abs. 1 UAbs. 1 lit. d. Hs. 2 KI-VO). Auf ein rein personenbezogenes Predictive Policing zielt § 40a ThürPAG-E nicht ab.

b. Anforderungen an Hochrisiko-KI-Systeme, Art. 6 ff. KI-VO

Die Software zur automatisierten Datenanalyse zählt (nur) dann zu Hochrisiko-KI-Systemen im Sinne von Art. 6 KI-VO, wenn sie zu bestimmten Einsatzzwecken im Bereich Strafverfolgung oder der straftatenbezogenen Gefahrenabwehr zum Einsatz kommt (Anhang III der KI-VO). Gem. Anhang III Nr. 6 der KI-VO zählen dazu im Bereich Strafverfolgung auch

- KI-Systeme zur Bewertung des Risikos einer Person, Opfer eines Verbrechens zu werden (Anhang III Nr. 6 lit. a)
- Systeme zur Bewertung des Risikos einer Person, straffällig zu werden oder erneut straffällig zu werden, die nicht nur auf der Grundlage eines Profils oder der Bewertung von Persönlichkeitsmerkmalen oder früherem kriminellen Verhalten beruhen (Anhang III Nr. 6 lit. d)
- Systeme zum Profiling bei der Ermittlung, Untersuchung oder Verfolgung von Straftaten (Anhang III Nr. 6 lit. e)

Insbesondere die in Anhang III Nr. 6 lit. d und lit. e KI-VO genannten Zwecke werden mit der automatisierten Datenanalyse zur Gefahrenabwehr berührt. Auch dürfte sich regelmäßig ein Profiling oder eine Risikoanalyse anschließen (Anhang III Nr. 6 lit. a). Daher sind KI-Systeme, die im Rahmen einer polizeilichen automatisierten Datenanalyse eingesetzt werden, regelmäßig als Hochrisiko-KI-Systeme einzustufen.³¹ Der Entwurf der Leitlinien der EU-Kommission zur Einstufung von Hochrisiko-KI enthält hierzu nähere Regelungen zur Abgrenzung von Systemen, die von nationalen Geheimdiensten eingesetzt werden.³²

c. Anbieterpflichten

Sicherheitsbehörden, die Hochrisiko-KI-Systeme verwenden, treffen als Anbieter und/oder Betreiber umfangreiche, auf die Produktsicherheit gerichtete Pflichten (Art. 8 ff. KI-VO).³³ Die KI-VO definiert Anbieter als Stelle, die „*ein KI-System [...] entwickelt oder entwickeln lässt und es unter ihrem eigenen Namen [...] in Verkehr bringt oder [...] in Betrieb nimmt*“ (Art. 3 Nr. 3 KI-VO). Betreiber ist wer ein KI-System in eigener Verantwortung verwendet (Art. 3 Nr. 4 KI-VO), unabhängig davon, ob die Stelle das KI-System auf eigenen Servern mit eigenem Personal betreibt oder es als „Software-as-a-Service“-Lösung nutzt.³⁴

³¹ Schöndorf-Haubold/Giorgios, KI im Einsatz für die Sicherheit: Innovation und Kontrolle im Spannungsfeld von europäischer Gesetzgebung und nationaler Souveränität, VerfBlog, 2024/12/10, <https://verfassungsblog.de/ki-im-einsatz-fur-die-sicherheit/> (Zugriff: 09.02.2026).

³² Entwurf über Leitlinien zur Einstufung von Hochrisiko-KI vom 19. Mai 2026, S. 111 ff., Ziff. Abs. 366 f. <https://digital-strategy.ec.europa.eu/de/library/draft-commission-guidelines-classification-high-risk-ai-systems> (Zugriff: 24.05.2026).

³³ Bäuerle ZD 2025, 128, 131; Martini/Botta, DÖV 2025, S. 1033, 1037.

³⁴ Martini/Botta, DÖV 2025, S. 1033, 1037.

Soweit die deutschen Sicherheitsbehörden derzeit noch keine Eigenentwicklungen verwenden und KI-Systeme von privaten Softwareunternehmen erwerben, sind sie daher derzeit grundsätzlich keine Anbieter iSv Art. 3 Nr. 3 KI-VO. Sie treffen jedoch die Pflichten von Quasi-Anbietern, wenn sie ein bereits in den Verkehr gebrachtes oder in Betrieb genommenes Hochrisiko-KI-System mit ihrem Namen versehen, Art. 25 Abs. 1 lit. a KI-VO, wie etwa „hesen-DATA“ usw. Dann treten diese Sicherheitsbehörden in die Anbieterrolle ein, und verdrängen den bisherigen Anbieter.³⁵ Hier müssen die Sicherheitsbehörden prüfen, ob der bisherige Anbieter die umfangreichen Pflichten der KI-VO beachtet hat und diese künftig auch selbst erfüllen.

Der Anbieter muss ein Risikomanagementsystem vorhalten, das Risiken über den gesamten Lebenszyklus des Systems identifiziert, Art. 9 KI-VO. Er muss für die Qualität der eingesetzten Trainings-, Validierungs- und Testdatensätze Sorge tragen, Art. 10 KI-VO. Den Anbieter tragen Dokumentationspflichten, Art. 11 KI-VO, sowie Protokollierungspflichten, Art. 12 KI-VO. Das Hochrisiko-KI-System ist transparent zu gestalten und es ist eine wirksame menschliche Aufsicht, Artt. 13, 14 KI-VO und eine hohe Systemzuverlässigkeit, Genauigkeit und Cybersicherheit sicher zu stellen, Art. 15 KI-VO. Es besteht eine Registrierungspflicht, Artt. 49, 71 Abs. 1 KI-VO. Bei Sicherheitsbehörden ist die Datenbank allerdings nicht-öffentlich, Art. 71 Abs. 4 KI-VO.

d. Betreiberpflichten

Verwenden Sicherheitsbehörden Hochrisiko-KI-Systeme, so treffen diese als Betreiber erhebliche Pflichten.³⁶ Gem. Art. 3 Nr. 4 KI-VO ist Betreiber, wer ein KI-System in eigener Verantwortung verwendet. Betreiber sind dazu verpflichtet, geeignete technische und organisatorische Maßnahmen zu ergreifen, um die Verwendung des Hochrisiko-KI-Systems nach Maßgabe der Betriebsanleitung sicherzustellen, Art. 26 Abs. 1 KI-VO, die menschliche Aufsicht einer natürlichen Person mit der erforderlichen Befähigung und Befugnis zu übertragen, Art. 26 Abs. 2 KI-VO, und sicherzustellen, dass die Eingabedaten relevant und ausreichend repräsentativ sind, Art. 26 Abs. 4 KI-VO. Natürliche Personen sind zu informieren, wenn ein Anhang-III-System die betreffenden Entscheidungen trifft oder bei solchen Entscheidungen zur Unterstützung verwendet wird, Art. 26 Abs. 11 KI-VO. Betreiber müssen den Betrieb des Systems zudem überwachen und den Anbieter informieren, wenn sie Grund zur Annahme haben, dass der Einsatz des Systems gemäß der Gebrauchsanweisung die Nonkonformität begründet, Art. 26 Abs. 5 KI-VO. Im Falle eines möglichen Risikos i.S.d. Art. 79 KI-VO ist die zuständige Marktüberwachungsbehörde in Kenntnis zu setzen. Für alle Hochrisiko-KI-Systeme gem. Art. 6 Abs. 2 i.V.m. Anhang III (mit Ausnahme III Ziff. 2 – kritische Infrastrukturen) ist von Polizei- und Strafverfolgungsbehörden eine Grundrechtfolgenabschätzung vorzunehmen, also eine Abschätzung der Auswirkungen, die die Verwendung auf die Grundrechte haben kann. Darin enthalten sein muss gem. Art. 27 KI-VO eine Beschreibung der Verfahren des Betreibers, bei denen das Hochrisiko-KI-System im Einklang mit seiner Zweckbestimmung verwendet wird, eine Beschreibung des Zeitraums und der Häufigkeit, innerhalb dessen bzw. mit der jedes Hochrisiko-KI-System verwendet werden soll, sowie die Katego-

³⁵ Martini/Botta, DÖV 2025, S. 1033, 1035.

³⁶ Vassel, EuZW 2024, S. 829, 831f.

rien der natürlichen Personen und Personengruppen, die von seiner Verwendung im spezifischen Kontext betroffen sein könnten. Der Betrieb von Hochrisiko-KI-Systemen durch Polizei- und Strafverfolgungsbehörden ist einer Registrierungspflicht unterworfen, Art. 26 Abs. 8 KI-VO, der Zugang (nichtöffentlicher Teil) ist auf die EU-Kommission sowie die Marktüberwachungsbehörden beschränkt, Art. 49 Abs. 4, 5 KI-VO. Polizei- und Strafverfolgungsbehörden, die KI-Systeme einsetzen, müssen zuvor für die KI-Kompetenz ihrer Bediensteten Sorge tragen. Gem. Art. 4 KI-VO haben diese Maßnahmen zu ergreifen, *„um nach besten Kräften sicherzustellen, dass ihr Personal und andere Personen, die in ihrem Auftrag mit dem Betrieb und der Nutzung von KI-Systemen befasst sind, über ein ausreichendes Maß an KI-Kompetenz verfügen, wobei ihre technischen Kenntnisse, ihre Erfahrung, ihre Ausbildung und Schulung und der Kontext, in dem die KI-Systeme eingesetzt werden sollen, sowie die Personen oder Personengruppen, bei denen die KI-Systeme eingesetzt werden sollen, zu berücksichtigen sind“*. Zu diesen Maßnahmen gehören die Entwicklung von internen Richtlinien und Standards, die Fortbildung und Schulung, Zertifizierungsprogramme, praxisorientiertes Lernen in divers zusammengesetzten Teams, die Ernennung von behördlichen KI-Beauftragten.³⁷ Nach der Übergangsregelung des Art. 111 Abs. 2 S. 2 KI-VO verbleibt dem mitgliedstaatlichen Gesetzgeber für die Umsetzung noch eine Übergangsfrist bis zum 2. August 2030.

Wie bereits unter „III. Prüfungsmaßstab“ dargestellt und vorliegend im konkreten Fall erläutert, harmonisiert die KI-VO also in unterschiedlicher Weise:

Bei den Hochrisiko-KI-Systemen behalten die Mitgliedstaaten einen weiten Gestaltungsspielraum bei der Schaffung von Befugnisnormen zu deren Einsatz.

Vollharmonisiert ist hingegen die Verwendung von Systemen iSv Art. 5 KI-VO (verbotene Systeme) und Art. 26 Abs. 10 KI-VO (Genehmigungspflicht von nachträglicher biometrischer Fernidentifizierung), was dazu führt, dass das BVerfG hier die Maßnahmen anhand Art. 7, 8 Grundrechtecharta zu prüfen hat.³⁸

IV. Grundgesetzlicher Rahmen

1. Rechtsprechung des BVerfG vom 16. Februar 2023

Mit Urteil vom 16. Februar 2023 hat das BVerfG die Ermächtigungsgrundlagen zur automatisierten Datenanalyse im Hessischen Polizeigesetz (§ 25a HSOG a.F.) sowie im Hamburgischen Gesetz über die Datenverarbeitung der Polizei (§ 49 HmbPolDVG a.F.) für verfassungswidrig erklärt. Nach Auffassung des Gerichts verstoßen die Regelungen gegen das allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG in seiner Ausprägung als Recht auf informationelle Selbstbestimmung.³⁹

Das Gericht stellt dabei zunächst klar, dass der Gesetzesvorbehalt nicht nur die erstmalige Erhebung personenbezogener Daten erfasst, sondern ebenso deren weitere Verarbeitung

³⁷ Wendehorst, in: Martini/Wendehorst (Hrsg.), KI-VO, 2. Aufl. 2026, Art. 4 Rn. 33ff.

³⁸ Hofmann-Coombe, EuR 2025, S. 363, 381; Zum Grundrechtsschutz bei harmonisiertem Polizeirecht auch Pfeffer, NVwZ 2022, 294, 297.; zu Harmonisierungstendenzen dies. NVwZ 2023, 1286, 1288f.

³⁹ BVerfG - 1 BvR 1547/19; 1 BvR 2634/20 Rn. 152 ff., Nr. 2 des Tenors.

und Zweckänderung.⁴⁰ Die automatisierte Analyse bereits rechtmäßig erhobener Daten stellt danach einen eigenständigen Grundrechtseingriff dar, der nicht durch die ursprüngliche Erhebungsbefugnis legitimiert wird, sondern einer eigenen, hinreichend bestimmten gesetzlichen Ermächtigungsgrundlage bedarf.⁴¹ Maßgeblich ist, dass durch die algorithmische Verknüpfung und Auswertung vorhandener Daten neues Wissen generiert wird, das Rückschlüsse auf betroffene Personen ermöglicht und qualitativ über den ursprünglichen Erhebungszusammenhang hinausgeht.⁴²

Das BVerfG bejaht den legitimen Zweck der automatisierten Datenanalyse ebenso wie deren grundsätzliche Geeignetheit und Erforderlichkeit zur vorbeugenden Bekämpfung schwerer Straftaten.⁴³ (Frage Nr. 93)

Verfassungsrechtlich entscheidend ist jedoch die Verhältnismäßigkeit im engeren Sinne. Diese hängt maßgeblich vom Gewicht des Grundrechtseingriffs ab, welches das Gericht bei der automatisierten Datenanalyse als besonders hoch einstuft.⁴⁴ Die besondere Eingriffsintensität ergibt sich nach Auffassung des Gerichts aus den der Maßnahme immanenten Belastungseffekten,⁴⁵ die unabhängig vom Gewicht der ursprünglichen Datenerhebung bestehen. Die automatisierte Zusammenführung umfangreicher und heterogener Datenbestände verleiht der Maßnahme ein eigenständiges „Eigengewicht“.⁴⁶ Dieses resultiert insbesondere aus der gesteigerten Effektivität polizeilicher Informationsverarbeitung, die es erlaubt, in kurzer Zeit komplexe Beziehungsgeflechte, Muster und Zusammenhänge zu erkennen oder überhaupt erst herzustellen.⁴⁷ Damit wirkt die automatisierte Datenanalyse regelmäßig vorgelagert zu weiteren polizeilichen Maßnahmen und beeinflusst die präventive Gefahrenprognose, von der wiederum die Reichweite nachfolgender Eingriffsbefugnisse abhängt.

Über dieses vom BVerfG hervorgehobene Eigengewicht hinaus ist jedoch zu berücksichtigen, dass die automatisierte Datenanalyse nicht lediglich einen einzelnen informationellen Grundrechtseingriff intensiviert, sondern strukturell auf die gesamte Architektur polizeilicher Eingriffsbefugnisse zurückwirkt.⁴⁸ Sie setzt nicht erst auf der Ebene konkreter Eingriffsmaßnahmen an, sondern betrifft die vorgelagerte Stufe der polizeilichen Gefahrenprognose selbst und verändert damit die tatsächliche Grundlage, von der aus über das Vorliegen gesetzlicher Gefahrenschwellen entschieden wird. Während klassische Gefahrenprognosen typischerweise auf einer begrenzten, durch menschliche Wahrnehmungs- und Kombinationsfähigkeiten geprägten Tatsachengrundlage beruhen, ermöglichen automatisierte Analyseverfahren die nahezu augenblickliche Verdichtung vorhandener Datenbestände sowie die Erzeugung neuer, komplexer Beziehungs- und

⁴⁰ BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 61.

⁴¹ BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20, Rn. 55; Weisser GSZ 2023, 183 (185).

⁴² BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 142.

⁴³ BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 52, 53.

⁴⁴ BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 59, 64.

⁴⁵ BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 66, 67.

⁴⁶ BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 67 ff. Ls. 3.

⁴⁷ BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 39.

⁴⁸ S. auch Lenschow, Eyk: Allwissende Polizei?: Entgrenzungen im Polizeirecht durch intelligente Gefahrenermittlung am Beispiel des SächsPVDG-E, VerfBlog, 2026/1/07, <https://verfassungsblog.de/polizeigesetz-sachsen-referentenentwurf/>, DOI: 10.59704/dc1ccce73bb2e95b (Abruf: 16.01.2026)

Verdachtslagen. Dadurch verschiebt sich das faktische Gewicht der Gefahreinschätzung, ohne dass der Gesetzgeber die formellen Eingriffsschwellen selbst angepasst hätte. Die Maßnahme wirkt insoweit entgrenzend, indem sie bestehende Schwellenwerte nicht normativ absenkt, sondern technologisch unterläuft. In dieser Perspektive ist die automatisierte Datenanalyse nicht nur als eigenständiger Grundrechtseingriff, sondern als strukturprägendes Instrument der polizeilichen Gefahrenabwehr zu begreifen.

Vor diesem Hintergrund betont das BVerfG, dass bestehende Eingriffsschwellen vielfach unter der Prämisse begrenzter menschlicher Auswertungs- und Kombinationsfähigkeiten entwickelt worden seien. Diese Annahme verliere angesichts moderner Analyseverfahren an Tragfähigkeit. In einer zunehmend datafizierten Gesellschaft bestehe daher die Gefahr einer strukturellen Ausweitung polizeilicher Eingriffsmöglichkeiten, sofern der Gesetzgeber dem nicht durch klare normative Begrenzungen entgegenwirkt.

Die angegriffenen Ermächtigungsgrundlagen aus Hamburg und Hessen genügten diesen Anforderungen nicht. Sie erlaubten eine daten- und methodenoffene Analyse polizeilicher Datenbestände, ohne Art, Umfang und Herkunft der einbezogenen Daten hinreichend zu bestimmen. Auch die tatbestandlichen Voraussetzungen der Maßnahme blieben zu unbestimmt.⁴⁹ Insbesondere genügten Formulierungen, die an einen „begründeten Einzelfall“ oder allgemein an die „vorbeugende Bekämpfung“ bestimmter Straftaten anknüpfen, nicht den verfassungsrechtlichen Anforderungen an eine tragfähige Eingriffsschwelle. Nach Auffassung des Gerichts muss die automatisierte Datenanalyse jedenfalls auf die Identifizierung einer zumindest konkretisierten Gefahr für besonders gewichtige Rechtsgüter gerichtet sein und auf solche Daten beschränkt werden, die zur Abwehr dieser Gefahr geeignet sind.⁵⁰

Zugleich zeigt das BVerfG auf, dass der Gesetzgeber das Eingriffsgewicht der automatisierten Datenanalyse durch verschiedene normative Stellgrößen steuern kann:

Die Anforderungen an die Ermächtigungsgrundlagen zur automatisierten Datenanalyse sind danach abhängig von Art und Umfang der verarbeitbaren Daten und der zugelassenen Methode der Datenanalyse oder -auswertung.⁵¹ Der Gesetzgeber kann die Eingriffsintensität in den Ermächtigungsgrundlagen danach zum einen über Tatbestandsvoraussetzungen steuern: Schwerwiegende Eingriffe in die informationelle Selbstbestimmung sind nur zum Schutz besonders gewichtiger Rechtsgüter möglich und sofern für diese eine zumindest hinreichend konkretisierte Gefahr besteht.⁵² Eine Ausnahme besteht, wenn die zugelassenen Analyse- und Auswertungsmöglichkeiten durch Regelungen insbesondere zur Begrenzung von Art und Umfang der Daten und zur Beschränkung der Datenverarbeitungsmethoden normenklar und hinreichend bestimmt sind, weil dadurch das Eingriffsgewicht der Maßnahmen erheblich gemindert ist.⁵³ Der Gesetzgeber kann schließlich durch Verfahrensanforderungen für Nachvollziehbarkeit, Transparenz und behördliche Kontrolle sorgen, wie etwa mit Pflichten zur

⁴⁹ BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 131, 165.

⁵⁰ BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 164 ff.

⁵¹ Dazu eingehend Kugelman/Buchmann, GSZ 2024, S. 1ff.

⁵² BVerfG, Urteil v. 1.10.2024 – 1 BvR 1160/19 Rn. 103 ff.

⁵³ Kugelman/Buchmann, GSZ 2024, S. 1, 8 f.

Kennzeichnung, Protokollierung oder Benachrichtigung.⁵⁴ Dabei gilt, je mehr Daten einbezogen werden (sensible Daten), desto weniger Zugriffsberechtigte sind zulässig. Hier sind Zugriffsbeschränkungen auf einen ausgewählten Kreis mit besonderer Qualifikation erforderlich.⁵⁵ Eine behördliche Kontrolle kann aber bei der automatisierten Datenanalyse wegen der hohen Anzahl von Verfahren nur über Stichproben durch Datenschutzbeauftragte erfolgen.⁵⁶ Das BVerfG hat mithin zahlreiche Faktoren aufgezeigt, über die das Eingriffsgewicht in die informationelle Selbstbestimmung durch den Gesetzgeber gesteuert werden kann, dem die Aufgabe obliegt, in der gesetzlichen Regelung ein angemessenes Verhältnis zwischen der Eingriffsschwelle und der bezweckten Gefahrenabwehr zu finden.⁵⁷

Außerdem kann der Gesetzgeber laut BVerfG die entsprechende Regelungsaufgabe auch zum Teil auf die Exekutive übertragen, wobei er die wesentlichen Grundlagen zur Begrenzung der Verarbeitungsmethoden und zur Art und Umfang der Daten selbst zu regeln hat, um dem Gesetzesvorbehalt zu entsprechen.⁵⁸

Automatisierte Datenanalysen im Polizeirecht sind danach nicht von vornherein ausgeschlossen, setzen jedoch eine präzise gesetzgeberische Entscheidung über Eingriffsschwelle, Datenumfang und Zweckbindung voraus. Die vom Bundesverfassungsgericht entwickelten Maßstäbe zwingen den Gesetzgeber damit zu einer Neubewertung bestehender polizeirechtlicher Ermächtigungsgrundlagen, in der die gesteigerte Leistungsfähigkeit algorithmischer Analyseinstrumente normativ reflektiert und durch hinreichend bestimmte Regelungen in ein angemessenes Verhältnis zum Grundrecht auf informationelle Selbstbestimmung gesetzt wird.

2. Einbeziehung privater Dienstleister (Frage 96)

Unter Berufung auf die verfassungsrechtlich gebotene digitale Souveränität weisen zahlreiche Kritiker derzeit darauf hin, dass bei der Einbeziehung privater Dienstleister im Bereich von eingriffsintensiven Maßnahmen größte Zurückhaltung geboten ist.⁵⁹ Die Konferenz der unabhängigen deutschen Datenschutzaufsichtsbehörden der Länder und des Bundes betonte nochmals im September 2025 im Hinblick auf den Einsatz von Software zur automatisierten Datenanalyse ausdrücklich, dass bei polizeilichen Datenbeständen eine Schutzpflicht gegenüber den Grundrechtsträgern besteht, dass Daten nicht ohne vorherige Prüfung in Drittstaaten weiterverwendet werden können, die hinter dem europäischen Rechtsstaatsniveau zurückbleiben. Darüber hinaus verlange die digitale Souveränität die Nachvollziehbarkeit und die Beherrschbarkeit der Datenverarbeitung, auch im Wege außergerichtlicher oder gerichtlicher Rechtsdurchsetzung, und die langfristige Vorhersehbarkeit und Verlässlichkeit des Angebots. Dies sei regelmäßig nur durch den Einsatz von Systemen erreichbar, deren Anbieter ihren Sitz im Europäischen Wirtschaftsraum (EWR) haben. Zur Wahrung der digitalen Souveränität durch Unterbindung von Abhängigkeiten sei sicherzustellen, dass die ein-

⁵⁴ BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 109; Kugelman/Buchmann, GSZ 2024, S. 1, 9f.

⁵⁵ Kugelman/Buchmann, GSZ 2024, S. 1, 9.

⁵⁶ BVerfG, Urteil vom 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 109; Kugelman/Buchmann, GSZ 2024, S. 1, 9.

⁵⁷ BVerfG, Urteil vom 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 103.

⁵⁸ BVerfG, Urteil vom 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 110, 112.

⁵⁹ Zum Ganzen Kelber/Bortnikov, NJW 2023, S. 2000 ff.; Bäuerle, ZD 2025, S. 128, 131.

gesetzten Systeme hinreichend offen sind, um nötigenfalls einen Wechsel auf ein geeignetes System zu ermöglichen.⁶⁰ In diesem Zusammenhang wird auch vollumfänglich auf die Ergebnisse des Rechtsgutachten im Auftrag des Bundesministeriums für Inneres und für Heimat vom 21. März 2025 verwiesen, wonach gemäß der US-Rechtslage ein weltweiter Datenzugriff durch US-Behörden bei Nutzung von Cloud-Diensten besteht.⁶¹

V. Automatisierte Datenanalyse durch Europol als „Service für die Sicherheitsbehörden der Mitgliedstaaten“

Im vorliegenden Zusammenhang ist auf Art. 18a VO (EU) 2022/991 hinzuweisen, wonach nationale Strafverfolgungsbehörden nunmehr Europol mit der Auswertung von Daten beauftragen können, sofern diese auch unter dem entsprechenden nationalen Rechtsrahmen in Ermittlungsverfahren ausgewertet und erhoben werden dürfen. Damit soll klargestellt werden, dass die Datenverarbeitung und Datenübermittlung möglich sind, solange sie den rechtlichen Anforderungen im jeweiligen Mitgliedsstaat genügen („Rechtmäßigkeitsfilter“).

Die automatisierte Datenanalyse wird vermehrt auch von den Europäischen Sicherheitsagenturen, wie etwa Europol eingesetzt.⁶² Der Austausch und die Analyse von kriminalpolizeilichen Informationen gehört zu den Kernaufgaben Euopols gem. Art. 88 Abs. 2, lit. a) AEUV. Europol hatte eine Analyse-Software automatisierten Datenanalyse eingesetzt,⁶³ bevor die VO (EU) 2022/991 einen Rechtsrahmen für die Verarbeitung und automatisierte Datenanalyse schuf. Hierdurch sollen Bezüge zu anderen Kriminalitätsbereichen oder zu Ermittlungen in anderen Mitgliedstaaten hergestellt werden (Art. 18 Abs. 6a). Mit der Regelung soll klargestellt werden, dass die Agentur eingehende Daten vorab analysieren und feststellen kann, ob diese unter eine der zulässigen Kategorien des (Art. 18) fallen. Die betreffenden Daten sollen dann auch mit bereits vorliegenden abgeglichen werden dürfen. Europol soll so grenzüberschreitende Querverbindungen erfassen, welche die nationalen Behörden so nicht selbst hätten feststellen können. Insgesamt wird nun ausdrücklich die Befugnis zur automatisierten Datenanalyse als Service für die Mitgliedstaaten⁶⁴ und andere EU-Agenturen geregelt: Europol soll danach nicht nur

⁶⁰ Die Konferenz der unabhängigen der unabhängigen deutschen Datenschutzaufsichtsbehörden der Länder und des Bundes, Pressemitteilung v. 18.9.2025 zur verfassungskonformen Ausgestaltung automatisierter Datenanalysen durch Polizeibehörden.

⁶¹ Rechtsgutachten zur US-Rechtslage zum weltweiten Datenzugriff durch US-Behörden bei Nutzung von Cloud-Diensten veröffentlicht unter <https://fragdenstaat.de/dokumente/273689-rechtsgutachten-zur-us-rechtslage-zum-weltweiten-datenzugriff-durch-us-behoerden-bei-nutzung-von-cloud-diensten/> (Zugriff: 24.05.2026).

⁶² Dazu Pfeffer, Die EU-Regulierung des KI-Einsatzes durch Sicherheitsbehörden - Zwischen nationaler Souveränität und Supranationalität, in: dies. (Hrsg.), AI and Policing in the Security Union – Chancen, Risiken und rechtliche Herausforderungen, Schriftenreihe der Forschungsstelle Europäisches und Deutsches Sicherheitsrecht (FEDS), Band 8, erscheint Anfang 2026.

⁶³ Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion DIE LINKE. – BT-Drs. 18/13194, Techniken zur Internetermittlung bei der Polizeiagentur Europol, BT-Drs. 18/13310, Antwort auf Frage 8; Vgl. ebenso: Antwort des Parlamentarischen Staatssekretärs Peter Tauber vom 26.04.2018 auf Anfrage des Abgeordneten Omid Nouripour (BÜNDNIS 90/DIE GRÜNEN), Frage 77 der Schriftlichen Fragen mit den in der Woche vom 30.04.2018 eingegangenen Antworten der Bundesregierung, BT-Drs. 19/1979.

⁶⁴ Die Bundesregierung hat den Entwurf eines Zweiten Gesetzes zur Änderung des Europol-Gesetzes vorgelegt, BT-Drs. 21/2373, v. 22.10.2025, welches innerstaatlich die Zuständigkeiten der beteiligten Behörden von Bund und Ländern

Daten über verurteilte Straftäter und Tatverdächtige verarbeiten dürfen, sondern auch über „Personen, in deren Fall nach Maßgabe des nationalen Rechts des betreffenden Mitgliedstaats faktische Anhaltspunkte oder triftige Gründe dafür vorliegen, dass sie Straftaten begehen werden, für die Europol zuständig ist.“

Am 18. Dezember 2025 hat der Bundestag die Änderung des Europol-Gesetzes beschlossen, um die deutsche Rechtslage an die geänderte VO (EU) 2022/991 anzupassen.⁶⁵ Der darin neu eingefügte Absatz 1a Satz 1 in § 3 des Europol-Gesetzes erweitert künftig innerstaatlich die Möglichkeit der Übermittlung von Informationen durch die zuständigen nationalen Behörden über das Bundeskriminalamt auf den neuen Artikel 18a der Europol-Verordnung.

Allerdings kann das neue Europol-Gesetz ausdrücklich nicht die materiellen und formellen Voraussetzungen und Bedingungen regeln, unter denen das Bundeskriminalamt, die Behörden der Bundespolizei und des Zolls, die weiteren Ermittlungsbehörden der Bundesfinanzverwaltung, die Polizeien der Länder sowie die mit der Steuerfahndung betrauten Dienststellen der Landesfinanzbehörden personenbezogene Daten an Europol übermitteln dürfen. Soweit diese Behörden Europol mit der automatisierten Datenanalyse beauftragen sollen, ist dafür zuvor eine Ermächtigungsgrundlage in den jeweiligen Fachgesetzen erforderlich.

Festzuhalten bleibt, dass mit der Schaffung der Ermächtigungsgrundlage für die automatisierte Datenanalyse in § 40a ThürPAG-E künftig auch Europol mit einer automatisierten Datenanalyse beauftragt werden kann.

Dass eine Ermächtigungsgrundlage einer Sicherheitsbehörde eines Mitgliedstaates zur automatisierten Datenanalyse geeignet ist, die Art und Weise der Durchführung einer automatisierten Datenanalyse durch eine europäischen Agentur, die die automatisierte Datenanalyse „als Service“ für eine mitgliedstaatliche Sicherheitsbehörde durchführt, einzuhegen, erscheint mangels Bindungswirkung im Verhältnis zu EU-Agenturen fraglich.

VI. Anmerkungen zur konkreten Ausgestaltung von § 40a ThürPAG-E

Während die KI-VO primär auf die Produktsicherheit gerichtete Verfahrensvorgaben enthält, also das „Wie“ des Einsatzes von KI-Systemen regelt, bleibt es in der Kompetenz der Mitgliedstaaten, das „Ob“ des Einsatzes zu regeln (siehe III. und VI.). Das „Ob“ des Einsatzes von Systemen zur automatisierten Datenanalyse durch Landespolizeien fällt in den Kompetenzbereich der Länder.

Ein legitimer Zweck der automatisierten Datenanalyse ist ebenso zu bejahen, wie deren grundsätzliche Geeignetheit und Erforderlichkeit zur vorbeugenden Bekämpfung schwerer Straftaten (dazu bereits unter IV.1, Frage 93)⁶⁶

Verfassungsrechtlich entscheidend ist jedoch die Verhältnismäßigkeit im engeren Sinne. Diese hängt maßgeblich vom Gewicht des Grundrechtseingriffs ab, welches das BVerfG bei

bezüglich der Zusammenarbeit mit Europol sowie die Beziehungen dieser Behörden im Verhältnis zueinander bei der Zusammenarbeit mit Europol regeln soll.

⁶⁵ Gesetzentwurf der Bundesregierung Entwurf eines Zweiten Gesetzes zur Änderung des Europol-Gesetzes Drs. BT 21/2373 vom 22.10.2025.

⁶⁶ BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 52, 53.

der automatisierten Datenanalyse als besonders hoch einstuft.⁶⁷ Der Gesetzgeber kann das Eingriffsgewicht der automatisierten Datenanalyse durch verschiedene normative Stellgrößen steuern (dazu bereits unter IV.1., Frage 94)

1. Eingriffsintensität

a. Art und Umfang der Daten

§ 40a Abs. 3 S. 1 ThürPAG-E zählt auf, welche der rechtmäßig erhobenen und gespeicherten Daten in die Analyse einbezogen werden: „Vorgangs- und Fallbearbeitungssysteme, elektronische Ermittlungs- und Kriminalaktensysteme, Informations- und Fahndungssysteme, Kommunikationssysteme, Einsatzleit- und Einsatzdokumentationssysteme“.

Die Regelung trägt wenig dazu bei, die Eingriffstiefe der Maßnahme abzumildern. Art und Umfang der Daten wird hier nur sehr wenig reduziert.

Als besonders weitreichend ist hier die Einbeziehung von Vorgangsdaten und Falldaten zu werten. Die Einbeziehung beider Datenkategorien erhöht den Umfang der Daten der Datenanalyse erheblich. Ein Vorgang umfasst regelmäßig die Unterlagen, die im Zusammenhang mit einer polizeilichen Tätigkeit über eine bestimmte Person, Sache oder sonstigen Gegenstand polizeilichen Handels geführt werden. In dem Vorgang werden Anzeigen, Ermittlungsberichte und Vermerke, die nicht nur Daten zu Verdächtigen, Beschuldigten oder sonstigen Anlasspersonen enthalten, aufgenommen, sondern etwa auch Daten zu Anzeigeerstatern, Hinweisgebern oder Zeugen. Unter die Vorgangsdaten fallen sowohl die Vorgangssachbearbeitungsdaten als auch die Vorgangsverwaltungsdaten. Hierdurch werden auch Personen, die nicht Verdächtige oder Beschuldigte i.S.d. Strafprozessrechts oder Nichtstörer i.S.d. Polizeirechts erfasst, wie Anzeigeerstatte, Hinweisgeber oder Zeugen.

Noch weiter gefasst ist die Kategorie Falldaten. Auch hier können zahlreiche Nichtstörer erfasst werden: Falldaten aus Fallbearbeitungssystemen sollen die polizeiliche Fallbearbeitung bei komplexen, fallübergreifenden Ermittlungen oder Strukturermittlungen unterstützen. Ein Fallbearbeitungssystem geht über die reine Verwaltung von Vorgangsdaten hinaus. Es ist ein auf die Aufhellung von Strukturen hin ausgerichtetes Werkzeug, das weniger personen- als vielmehr ereignisbezogen ausgerichtet ist und vor allem Beziehungen zwischen Personen, Institutionen, Objekten und Sachen aufzeigen kann und sowohl für präventive als auch repressive Zwecke eingesetzt werden kann.

§ 40a Abs. 2 Satz 1 ThürPAG-E erlaubt die Einbeziehung von Daten aus „Kommunikationssystemen“ und „Informationssystemen“. Es handelt sich ebenfalls um eine sehr weite Formulierung. Hiernach kommt die Analyse von staatliche Registern in Betracht, wie Melde- oder Waffenregister oder das zentrale Verkehrsinformationssystem (ZEVIS).

⁶⁷ BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 59, 64.

Dem Wortlaut nach wären hier auch Internetquellen umfasst, deren Analyse ist jedoch in § 40a Abs. 5 Ziff. 3 ThürPAG-E gesondert behandelt, indem deren Analyse explizit ausgeschlossen wurde.

Die Verarbeitung von bestimmten Daten, die durch besonders schwere Grundrechtseingriffe erlangt wurden, z.B. durch die Wohnraumüberwachung oder den Einsatz verdeckter Ermittler, wird durch § 40a Abs. 1 S. 2 ThürPAG-E nur erlaubt zur Abwehr einer dringenden Gefahr für die hochrangigen Rechtsgüter nach § 40a Abs. 1 S. 1 ThürPAG-E. Gem. § 40a Abs. 2 S. 2 ThürPAG-E ist die Einbeziehung solcher Daten für Maßnahmen nach § 40a Abs. 2 S. 1 ThürPAG-E (Verhütung und Unterbindung von schweren Straftaten) ausgeschlossen (dazu näher unten VI.2.).

Voraussetzung einer begrenzenden Wirkung von Vorgaben zu Art und Umfang der Daten ist zunächst, dass die betroffenen personenbezogenen Daten gekennzeichnet werden.⁶⁸

Der Gesetzgeber kann durch Verfahrensanforderungen für Nachvollziehbarkeit, Transparenz und behördliche Kontrolle sorgen, wie etwa mit Pflichten zur Kennzeichnung, Protokollierung oder Benachrichtigung.⁶⁹ Dabei gilt, je mehr Daten einbezogen werden (sensible Daten), desto weniger Zugriffsberechtigte sind zulässig. Hier sind Zugriffsbeschränkungen auf einen ausgewählten Kreis mit besonderer Qualifikation erforderlich.⁷⁰ Eine behördliche Kontrolle kann aber bei der automatisierten Datenanalyse wegen der hohen Anzahl von Verfahren nur über Stichproben durch Datenschutzbeauftragte erfolgen.⁷¹

§ 40a Abs. 4 Satz 2 ThürPAG-E überlässt die Festlegung zur Kategorisierung und Kennzeichnung personenbezogener Daten der Exekutive. Ein Konzept der Kategorisierung und Kennzeichnung personenbezogener Daten und konkrete Regelungen, welche personenbezogenen Daten in welcher Weise in die automatisierte Analyse einbezogen werden dürfen, erfolgt in § 40a ThürPAG-E nicht. Ein Ausschluss personenbezogener Daten von Unbeteiligten/Nichtstörern erfolgt damit nicht auf parlamentsgesetzlicher Ebene. Auch eine einschränkende Regelung zu den zugelassenen Datenarten (vgl. etwa § 3 Abs. 1 ATDG oder § 29 Abs. 2a S. 3 GwG) findet sich in § 40a ThürPAG-E selbst nicht.⁷² Eingrenzende Regelungen zu Dateiformaten, z.B. Bilder, Video- und Audioaufnahmen, oder zum Ausschluss biometrischer Daten fehlen in § 40a ThürPAG-E.

Eine Abschwächung der Intensität des Eingriffs durch die Begrenzung auf bestimmte Datenarten könnte hier daher nur noch über eine Verwaltungsvorschrift erfolgen. Zwar kann der Gesetzgeber laut BVerfG die entsprechende Regelungsaufgabe zum Teil auf die Exekutive übertragen. Er muss aber die wesentlichen Grundlagen zur Begrenzung der Verarbeitungsmethoden und von Art und Umfang der Daten selbst regeln, um dem Gesetzesvorbehalt zu

⁶⁸ Ebenso Botta zum ASOG-E, Stellungnahme zum Entwurf eines Gesetzes zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin 26.09.2025, S. 14.

⁶⁹ BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 109; Kugelman/Buchmann, GSZ 2024, S. 1, 9f.

⁷⁰ Kugelman/Buchmann, GSZ 2024, S. 1, 9.

⁷¹ BVerfG, Urteil vom 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 109; Kugelman/Buchmann, GSZ 2024, S. 1, 9.

⁷² Ebenso Botta zum ASOG-E, Stellungnahme zum Entwurf eines Gesetzes zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin 26.09.2025, S. 13

entsprechen.⁷³ Überträgt der Gesetzgeber der Verwaltung näheres zu regeln, ist eine Verordnungsermächtigung vorzugswürdig.⁷⁴

Eingriffsmildernd ist der ausdrückliche Ausschluss einer direkten Anbindung der Analyseplattform an „der Allgemeinheit offenstehende Netzwerke“, etwa Internetdienste, in § 40a Abs. 5 Ziff. 3 ThürPAG-E.

Die Eingriffsintensität hätte auch durch eine Beschränkung der Herkunft der Daten auf solche, die ursprünglich durch inländische Polizeibehörden erhoben worden sind, vorgenommen werden können. Dies ist in § 40a ThürPAG-E aber nicht erfolgt. Somit könnten auch personenbezogene Daten, die von Geheimdiensten oder von anderen Sicherheitsbehörden der Mitgliedstaaten oder aber von Europäischen Sicherheitsagenturen (wie Europol oder Eurojust) an Polizeibehörden übermittelt wurden und sich somit nunmehr in den polizeilichen Datenbeständen befinden, in eine Analyseplattform nach § 40a ThürPAG-E einbezogen werden.

b. Einsatz lernender Systeme im Vorfeld konkretisierter Gefahren

Laut BVerfG verbietet das Grundgesetz lernende Systeme nicht generell.⁷⁵ Weil bei selbstlernenden Systemen die Gefahr besteht, dass die demokratische Legitimationskette zwischen Wahlvolk und Amtswalter und dessen Entscheidungsfindung durchbrochen wird (Demokratieprinzip, Art. 20 Abs. 1, 2 GG), sind dem Einsatz enge Grenzen gesetzt.

In der Literatur wurde angemerkt, dass die technologiebezogenen Aussagen des BVerfG aus dem Jahr 2023 möglicherweise noch unpräzise waren und das Gericht möglicherweise nicht zwischen Echtzeitlernmodellen und fixierten Modellen unterschieden hat. Es könne der Eindruck entstehen, das BVerfG habe nur zu Echtzeitlernmodellen urteilen wollen.⁷⁶

Unabhängig davon war das BVerfG jedenfalls sehr klar bei der Forderung, dass der Gesetzgeber beim Einsatz einer automatisierten Datenanalyse im Vorfeld einer konkretisierten Gefahr selbstlernende Systeme auszuschließen hat: „Wenn der Gesetzgeber die Eingriffsintensität [...] reduzieren will, um [die Datenanalyse] auch im Vorfeld einer konkretisierten Gefahr einsetzen zu können, muss er einschränkende Vorgaben zur Methode [...] machen. Der Einsatz selbstlernender Systeme muss dafür im Gesetz ausdrücklich ausgeschlossen sein.“⁷⁷ § 40a Abs. 5 Ziff. 2 ThürPAG-E schließt den Einsatz selbstlernender Systeme generell aus.

§ 40a Abs. 5 Ziff. 1 ThürPAG-E schließt eine automatisierte Entscheidungsfindung aus. Vor dem Hintergrund der Gewährleistung der Menschenwürde (Art. 1 Abs. 1 GG) und dem Demokratieprinzip (Art. 20 Abs. 1, 2 GG) ist es zu begrüßen, dass die Landesregierung das Letztentscheidungsgebot ausdrücklich verankert.⁷⁸ Wegen der Grundrechtsbindung gem.

⁷³ BVerfG, Urteil vom 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 110, 112.

⁷⁴ BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 113.

⁷⁵ BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 100.

⁷⁶ Etwa Kostov, Der Staat, 64 (2025) 4: 537, 574 f. mit Verweis auf BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 100.

⁷⁷ BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 120f.

⁷⁸ Martini/Botta DÖV 2025, 1033, 1042 zu § 47 Abs. 1 Satz 3 PolG BW.

Art. 1 Abs. 3 GG und dem Rechtsstaatsprinzip in Art. 20 Abs. 3 GG muss der Staat sicherstellen, dass staatliche Entscheidungsprozesse nachvollziehbar sind. Die Exekutive könnte ihre Entscheidungen sonst auch nicht hinreichend begründen.⁷⁹

Das Eingriffsgewicht sinkt, je „geschlossener“ die Methode des Suchvorgangs ist und je stärker die automatisierte Datenanalyse durch polizeiliche Suchmuster gesteuert wird, die auf spezifischen Erkenntnissen und Annahmen zum konkreten Sachverhalt beruhen.⁸⁰ In § 40a Abs. 3 Satz 2 THürPAG-E heißt es: „Die Anzeige der Ergebnisse ist technisch auf mit den Suchparametern übereinstimmende Treffer zu begrenzen.“ Hierdurch wird das Eingriffsgewicht abgesenkt.

Offen läßt der Gesetzgeber, wie diskriminierende Algorithmen verhindert werden und die die Nachvollziehbarkeit sichergestellt werden sollen.

c. Zwischenergebnis

Der Entwurf schwächt nur an wenigen Stellen die Eingriffsintensität der Maßnahme ab.

Ein ganz neuer Eingriff von besonderer Eingriffsintensität bestünde im Anlegen einer neuen vorsorglichen „Superdatenbank“. Mangels verfassungsrechtlicher Rechtfertigung wäre die derzeitige Regelung bereits deshalb verfassungswidrig. Sollte das Anlegen einer vorsorglichen Datenbank gar nicht beabsichtigt sein, müsste dies in der Norm noch klargestellt werden.

Die wesentlichen Leitplanken für Verfahren zur Durchführung der automatisierten Datenanalyse sind durch die Legislative selbst festzulegen. Diese fehlen im Entwurf des § 40a ThürPAG-E.

2. Tatbestand

Schwerwiegende Eingriffe in die informationelle Selbstbestimmung, wie die automatisierte Datenanalyse, sind nur zum Schutz besonders gewichtiger Rechtsgüter möglich und sofern für diese eine zumindest hinreichend konkretisierte Gefahr besteht.⁸¹

Der Tatbestand des § 40a Abs. 1 S. 1 ThürPAG-E erfüllt diese Anforderungen, denn er erlaubt eine Datenanalyse zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes, für Leib, Leben, Freiheit oder einer Person oder für oder für Anlagen der kritischen Infrastruktur oder sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen. Die Ermächtigungsgrundlage ist somit verfassungskonform.

Nach § 40a Abs. 2 S. 1 ThürPAG-E kann die automatisierte Datenanalyse auch „zur Verhütung oder Unterbindung von besonders schweren Straftaten“ erfolgen, „wenn aufgrund tatsächlicher Anhaltspunkte innerhalb eines übersehbaren Zeitraums mit weiteren gleichgelagerten Straftaten zu rechnen ist“.

⁷⁹ Martini/Botta DÖV 2025, 1033, 1042.

⁸⁰ BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 164 ff.

Da die vorbeugende Bekämpfung von Straftaten nicht mehr nur die Abwehr zukünftiger Schäden, sondern die Sicherung von Beweismitteln für künftige Strafverfahren betrifft, fällt diese Form der Strafverfolgungsvorsorge grundsätzlich in die Gesetzgebungskompetenz des Bundes Art. 74 I Nr. 1 GG und nicht des Landes. Laut BVerfG ist eine präventive automatisierte Datenanalyse hier aber ausnahmsweise erlaubt, wenn der Gesetzgeber durch qualitative Beschränkungen (Ausschluss sensibler Daten, limitierte Analyseverfahren) das Eingewicht des Eingriffs mindert oder aber die Maßnahme auf hinreichend konkretisierte Gefahren begrenzt.⁸² Andernfalls müsste hier eine Eingriffsschwelle greifen, die dem repressiven Instrumentarium entspricht – richterlicher Vorbehalt, Benachrichtigungspflichten und strenge Dokumentation eingeschlossen (Frage 104).

In § 40a Abs. 2 S. 1 ThürPAG-E erlaubt die automatisierte Dateneanalyse „zur Verhütung oder Unterbindung von besonders schweren Straftaten“, „wenn aufgrund tatsächlicher Anhaltspunkte innerhalb eines übersehbaren Zeitraums mit weiteren gleichgelagerten Straftaten zu rechnen ist“. Eine hinreichend konkretisierte Gefahr als Eingriffsschwelle, wie sie vom BVerfG formuliert wurde, dürfte damit nicht geregelt werden.⁸³ Allerdings erfolgt für diese Maßnahme gem. § 40a Abs. 2 S. 2 ThürPAG-E eine qualitative Beschränkung der zu analysierenden Daten, d.h. der Ausschluss von „DNA-Identifizierungsmustern, Finger- und Handflächenabdrücken, von Audio- und Videodateien oder von personenbezogenen Daten, die durch den Einsatz technischer Mittel in oder aus Wohnungen oder durch verdeckten Zugriff auf informationstechnische Systeme erhoben wurden.“ Für die Anordnung von Maßnahmen nach § 40a Abs. 2 S. 1 ThürPAG-E soll zudem § 34 Abs. 5 ThürPAG entsprechend geltend, wonach eine Anordnung durch die Leitung der Landespolizeidirektion oder des Landeskriminalamts oder einen von diesen besonders beauftragten Beamten des höheren Polizeivollzugsdienstes notwendig ist, vgl. § 34 Abs. 5 S. 1 ThürPAG. Auch § 34 Abs. 4 S. 4, 5 ThürPAG soll hier entsprechend Anwendung finden: Danach muss die Anordnung „schriftlich unter Angabe der für sie maßgeblichen Gründe zu erfolgen und ist auf höchstens drei Monate zu befristen. Eine Verlängerung um jeweils nicht mehr als drei weitere Monate ist zulässig, soweit die Voraussetzungen unter Berücksichtigung der gewonnenen Erkenntnisse fortbestehen.“. Der Ausschluss bestimmter Datenkategorien und der Anordnungsvorbehalt vermindern somit das Eingriffsgewicht iSd Rechtsprechung des BVerfG.

3. Verfahrensanforderungen zum Zwecke der Nachvollziehbarkeit, Transparenz und behördlichen Kontrolle (Frage 97)

Wie unter IV. 1 dargestellt, kann der Gesetzgeber durch Verfahrensanforderungen für Nachvollziehbarkeit, Transparenz und behördliche Kontrolle sorgen, wie etwa mit Pflichten zur Kennzeichnung, Protokollierung oder Benachrichtigung.⁸⁴ Dabei gilt, je mehr Daten einbezogen werden (sensible Daten), desto weniger Zugriffsberechtigte sind zulässig. Hier sind Zugriffsbeschränkungen auf einen ausgewählten Kreis mit besonderer Qualifikation erforderlich.⁸⁵ § 40a Abs. 4 Satz 1 ThürPAG-E regelt nur, dass das eingesetzte Personal besonders auszuwählen und zu schulen ist, das „wie“ wird nicht geregelt.

⁸² BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 47 ff.

⁸³ BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 107; 167f.

⁸⁴ BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 109; Kugelman/Buchmann, GSZ 2024, S. 1, 9f.

⁸⁵ Kugelman/Buchmann, GSZ 2024, S. 1, 9.

§ 40a Abs. 4 Satz 2 ThürPAG-E regelt lediglich, dass durch „technische und organisatorische Maßnahmen“ sicherzustellen ist, dass „die Zugriffsmöglichkeiten des eingesetzten Personals auf die zur Verfügung stehenden personenbezogenen Daten auf das erforderliche Maß“ beschränkt werden. Die Regelung näherer Verfahrensanforderungen wird im vorliegenden Gesetzesentwurf der Exekutive überlassen (Verwaltungsvorschriften). Im Sinne der Wesentlichkeitstheorie sind wesentliche Bestimmungen aber von der Legislative zu treffen.

VII. Fazit

Die Landesregierung schlägt mit ihrem Gesetzesentwurf eine Modernisierung des Thüringischen Polizeiaufgabengesetzes vor. Soweit hier betrachtet, ist der Gesetzesentwurf auch von dem Anspruch geprägt, die Effektivität der Gefahrenabwehr zu erhöhen, insbesondere auf die rasante Fortentwicklung der Datafizierung der Polizeiarbeit zu reagieren und zugleich das Verfassungs- und Unionsrecht zu beachten.

In einigen Punkten besteht bei der hier betrachteten Ermächtigungsgrundlage zur automatisierten Datenanalyse (§ 40a ThürPAG-E) noch Nachbesserungsbedarf. Ich empfehle den Entwurf insoweit entsprechend anzupassen.



Prof. Dr. iur. Kristin Pfeffer