

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

An den Vorsitzenden des
Innen- und Rechtsausschusses
Jan Kürschner
Schleswig-Holsteinischer Landtag
Landeshaus,
Düsternbrooker Weg 70
24105 Kiel



Akademie
POLIZEI Hamburg

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

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

Vorab per Email

Schleswig-Holsteinischer Landtag
Umdruck 20/7101

Hamburg, 3. September 2026

Gesetz zur Fortentwicklung polizeirechtlicher Maßnahmen für einen wirksamen Schutz der öffentlichen Sicherheit Gesetzentwurf der Landesregierung – Drucksache 20/4284 und Änderungsantrag, Umdruck 20/6786

Sehr geehrte Damen und Herren Abgeordnete,

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

Mit freundlichen Grüßen

gez.

Kristin Pfeffer

Stellungnahme

Gesetz zur Fortentwicklung polizeirechtlicher Maßnahmen für einen wirksamen Schutz der öffentlichen Sicherheit - Gesetzentwurf der Landesregierung – Drucksache 20/4284 und Änderungsantrag, Umdruck 20/6786

I. Vorbemerkung

Mit ihrem Gesetzesentwurf zur Fortentwicklung polizeirechtlicher Maßnahmen für einen wirksamen Schutz der öffentlichen Sicherheit im Lande Schleswig-Holstein sowie dem Änderungsantrag schlägt die Landesregierung neue Eingriffsbefugnisse für die Polizei vor, die erkennbar von dem Anspruch geprägt sind,

- die Effektivität der Arbeit der Polizei 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), sowie die zwischenzeitlich ergangenen Entscheidungen des BVerfG von 2023 umzusetzen.

Die nachfolgende Stellungnahme beschränkt sich auf einige Anmerkungen zu dem Regelungsvorschlag in § 188c LVwG-E (IT-gestützter Abgleich; Datenanalyse) und § 188d LVwG-E (Durchführung des IT-gestützten Abgleichs und der Datenanalyse). Die Vorschrift des § 188c LVwG-E führt zwei Maßnahmen zur Weiterverarbeitung verfügbarer personenbezogener Daten ein, den IT-gestützten Abgleich und die automatisierten Datenanalyse. Meine Ausführungen werden (nur) die automatisierte Datenanalyse betreffen.

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 hin zu

¹ Pfeffer, Wie europäisch wird deutsches Polizeirecht?: Wie über das Datenschutzrecht die Europäisierung des Polizeirechts betrieben wird, VerfBlog, 2021/4/28, <https://verfassungsblog.de/wie-europaisch-wird-deutsches-polizeirecht/>, DOI: 10.17176/20210428-173145-0 (Zugriff: 02.09.2026)

einer Harmonisierung des Sicherheitsrechts vollzogen.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:

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 regelmäßige 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 dabei aber die

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

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, VerfBlog, 2024/12/10, <https://verfassungsblog.de/ki-im-einsatz-fur-die-sicherheit/> (Zugriff: 12.08.2026).

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

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 zur Gefahrenabwehr und Strafverfolgung sowohl nach der DSRL-JI, als auch nach der KI-VO nach wie vor ein substanzieller Spielraum (Teilharmonisierung), so dass hier der Prüfungsmaßstab das Grundgesetz und nicht die Charta der Grundrechte bleibt.¹² Daneben sind die 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 werden (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) vorzusehen. Insbesondere besteht die Pflicht der Behörden, über die (mögliche) Datenverarbeitung mittels automatisierter Analyse zu informieren (Art. 13 DSRL-JI). Diese Anforderungen wurden im allgemeinen Datenschutzrecht von Bund und Ländern bereits umgesetzt. Eine 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 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 und Förderung der Technologie unter gleichzeitiger Beachtung der Grundrechte, Art. 1 Abs. 1 KI-VO.

Zwischenzeitlich, am 26. Juli 2026, ist der sog. „Digitale Omnibus“ für KI, eine Verordnung zur Änderung der KI-VO (Verordnung EU 2026/1744 vom 8. Juli 2026) in Kraft getreten, nach der die Anforderungen in der bisher geltenden KI-VO im Bereich Hochrisiko-KI wieder abgeschwächt werden. Mit dem „Digitalen Omnibus zu KI“ werden nun insbesondere die Fristen für die Geltung verschiedener Vorschriften in der KI-VO nach hinten verschoben. Für eigenständige Hochrisiko-KI gilt die KI-VO danach erst ab dem 2. Dezember 2027 (statt zuvor ab dem 2. August 2026). Außerdem wurden u.a. die Anforderungen an die sog. KI-Kompetenz der Betreiber abgeschwächt (dazu näher unter III.2.d).

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 essenziellen Bedeutung des Rechts der Inneren Sicherheit für die Souveränität eines Staates¹⁷ nach wie vor umstritten.¹⁸ 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.

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

¹⁸ BR-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/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: 12.08.2026).

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.¹⁹ Die Bekämpfung schwerer Kriminalität wird vom EuGH dagegen (nur) unter den Begriff „innere Sicherheit“ subsumiert.²⁰

Soweit § 188c Abs. 3 Satz 2 Ziff. 1 LVwG-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 ist zu beachten, 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,²¹ 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.²²

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

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

²⁰ EuGH 5.4.2022 – C-140/20 – Commissioner of An Garda Síochána. Zum Trennungsprinzip zwischen Polizei und Geheimdiensten Denninger, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, B. Rn. 43ff.; Zur grundsätzlichen Aufgabentrennung von Polizei und Militär Weingärtner, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, I. Rn. 679ff; Zu den Konflikten bei der Auslegung des Begriffs nationale Sicherheit Pfeffer, NVwZ 2023, S. 1288.

²¹ Dazu statt vieler Graulich, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, E. Rn. 221 ff.

²² 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: 12.08.2026).

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 inakzeptabel 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.²³ Die EU-Kommission hat zu den verbotenen Praktiken inzwischen Leitlinien im Sinne von Art. 96 Abs. 1 lit. b der KI-VO erarbeitet.²⁴

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 Zwecken 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.²⁵ 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.²⁶

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).²⁷

²³ Wendehorst, in: Martini/Wendehorst (Hrsg.), KI-VO, 2. Aufl. 2026, Art. 5 Rn. 2.

²⁴ 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 12.08.2026).

²⁵ 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: 12.08.2026).

²⁶ 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: 12.08.2026).

²⁷ Bäuerle ZD 2025, 128, 131; Martini/Botta, DÖV 2025, S. 1033, 1037.

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.²⁸

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 „hessen-DATA“ usw. Dann treten diese Sicherheitsbehörden in die Anbieterrolle ein und verdrängen den bisherigen Anbieter.²⁹ 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 treffen 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.³⁰ 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 von III Ziff. 2 – kritische Infra-

²⁸ Martini/Botta, DÖV 2025, S. 1033, 1037.

²⁹ Martini/Botta, DÖV 2025, S. 1033, 1035.

³⁰ Vasel, EuZW 2024, S. 829, 831f.

strukturen) 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 Kategorien 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. Gem. Art. 4 KI-VO müssen Anbieter und Betreiber von KI-Systemen Maßnahmen ergreifen, um die Entwicklung der KI-Kompetenz ihres Personals und anderer Personen „zu unterstützen“.

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 der Art. 7, 8 Grundrechtecharta zu prüfen hat.³¹

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.³²

Das Gericht stellt dabei zunächst klar, dass der Gesetzesvorbehalt nicht nur die erstmalige Erhebung personenbezogener Daten erfasst, sondern ebenso deren weitere Verarbeitung und Zweckänderung.³³ 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

³¹ 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.

³² BVerfG - 1 BvR 1547/19; 1 BvR 2634/20 Rn. 152 ff., Nr. 2 des Tenors.

³³ BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 61.

bestimmten gesetzlichen Ermächtigungsgrundlage bedarf.³⁴ 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.³⁵

Das BVerfG bejaht den legitimen Zweck der automatisierten Datenanalyse ebenso wie deren grundsätzliche Geeignetheit und Erforderlichkeit zur vorbeugenden Bekämpfung schwerer Straftaten.³⁶

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.³⁷ Die besondere Eingriffsintensität ergibt sich nach Auffassung des Gerichts aus den der Maßnahme immanenten Belastungseffekten,³⁸ die unabhängig vom Gewicht der ursprünglichen Datenerhebung bestehen. Die automatisierte Zusammenführung umfangreicher und heterogener Datenbestände verleiht der Maßnahme ein eigenständiges „Eigengewicht“.³⁹ 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.⁴⁰ 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.⁴¹ 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 Verdachtslagen. Dadurch verschiebt sich das faktische Gewicht der Gefahreneinschätzung, ohne dass der Gesetzgeber die formellen Eingriffsschwellen selbst angepasst hätte. Die

³⁴ BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20, Rn. 55; Weisser GSZ 2023, 183 (185).

³⁵ BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 142.

³⁶ BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 52, 53.

³⁷ BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 59, 64.

³⁸ BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 66, 67.

³⁹ BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 67 ff. Ls. 3.

⁴⁰ BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 39.

⁴¹ Pfeffer, Die neue DNA des Polizeirechts: Automatisierte Datenanalyse als verfassungsrechtliche Herausforderung, VerfBlog, 2026/9/02, <https://verfassungsblog.de/palantir-europarecht-verfassungsrecht/>, DOI: 10.59704/acb08b1635715b8f.; ähnlich Lenschow, Eyk: Allwissende Polizei?: Entgrenzungen im Polizeirecht durch intelligente Gefahrenermittlung am Beispiel des SächsPVDG-E, VerfBlog, 2026/1/07, <https://verfassungsblog.de/polizei-gesetz-sachsen-referentenentwurf/>, DOI: 10.59704/dc1ccce73bb2e95b (Abruf: 2.09.2026)

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.⁴² 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.⁴³

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.⁴⁴ 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.⁴⁵ 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.⁴⁶ Der Gesetzgeber kann schließlich durch Verfahrensanforderungen für Nachvollziehbarkeit, Transparenz und behördliche Kontrolle sorgen, wie etwa mit Pflichten zur

⁴² BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 131, 165.

⁴³ BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 164 ff.

⁴⁴ Dazu eingehend Kugelman/Buchmann, GSZ 2024, S. 1ff.

⁴⁵ BVerfG, Urteil v. 1.10.2024 – 1 BvR 1160/19 Rn. 103 ff.

⁴⁶ Kugelman/Buchmann, GSZ 2024, S. 1, 8 f.

Kennzeichnung, Protokollierung oder Benachrichtigung.⁴⁷ Dabei gilt, je mehr Daten einbezogen werden (oder auch sensible Daten), desto weniger Zugriffsberechtigte sind zulässig. Hier sind Zugriffsbeschränkungen auf einen ausgewählten Kreis mit besonderer Qualifikation erforderlich.⁴⁸ Eine behördliche Kontrolle kann aber bei der automatisierten Datenanalyse wegen der hohen Anzahl von Verfahren nur über Stichproben durch Datenschutzbeauftragte erfolgen.⁴⁹

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.⁵⁰

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 zu Art und Umfang der Daten selbst zu regeln hat, um dem Gesetzesvorbehalt zu entsprechen.⁵¹

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

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.⁵² Die EU-Mitgliedstaaten haben am 18. November 2025 die Declaration for European Digital Sovereignty unterzeichnet, wonach Abhängigkeiten zu reduzieren und gemeinsame demokratische Werte

⁴⁷ BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 109; Kugelman/Buchmann, GSZ 2024, S. 1, 9f.

⁴⁸ Kugelman/Buchmann, GSZ 2024, S. 1, 9.

⁴⁹ BVerfG, Urteil vom 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 109; Kugelman/Buchmann, GSZ 2024, S. 1, 9.

⁵⁰ BVerfG, Urteil vom 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 103.

⁵¹ BVerfG, Urteil vom 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 110, 112.

⁵² Zum Ganzen Bäuerle, ZD 2025, S. 128, 131; Esposito/Egbert, Palantir und digitale Souveränität, VerfBlog, 2026/8/26, <https://verfassungsblog.de/palantir-und-digitale-souveranitat/>, DOI: 10.59704/70233c5f9182b075. Kelber, Gläserne Bürger:innen, abhängiger Staat: Wie Palantir & Co. Macht verschieben – und was digitale Souveränität und Rechtsstaatlichkeit verlangen, VerfBlog, 2026/8/28, <https://verfassungsblog.de/palantir-polizei-datenschutz-sicherheit/>, DOI: 10.59704/54e6a67d0522382f.; ders./Bortnikov, NJW 2023, S. 2000 ff.; Nemitz, Die Waffen des Silicon Valley: Eine Kritik an Alex Karp's Manifest der digitalen Gewalt, VerfBlog, 2026/8/27, <https://verfassungsblog.de/palantir-manifest/>, DOI: 10.59704/88f05b5989b2ded0; Nicklas, Unwissen schützt vor Verantwortung nicht: Palantir im Staatsorganisationsrecht, VerfBlog, 2026/8/28, <https://verfassungsblog.de/palantir-staatsorganisationsrecht/>, DOI: 10.59704/180c83f8fe752815; Ruschemeier/Mühlhoff, Ein neues Betriebssystem des Staates: Warum Palantir rechtsstaatliche Strukturen verändert, VerfBlog, 2026/9/03, <https://verfassungsblog.de/palantir-machtanspruch/>, DOI: 10.59704/540a9b8960e14eea (Zugriff: 3.9.2026)

im digitalen Raum zu schützen sind. 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 und 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 eingesetzten Systeme hinreichend offen sind, um nötigenfalls einen Wechsel auf ein geeigneteres System zu ermöglichen.⁵³ 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.⁵⁴

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 Mitgliedstaat genügen („Rechtmäßigkeitsfilter“).

Die automatisierte Datenanalyse wird vermehrt auch von den Europäischen Sicherheitsagenturen, wie etwa Europol, eingesetzt.⁵⁵ Der Austausch und die Analyse von kriminalpolizeilichen Informationen gehören zu den Kernaufgaben Euopols gem. Art. 88 Abs. 2, lit. a) AEUV. Europol hatte eine Analyse-Software zur automatisierten Datenanalyse eingesetzt,⁵⁶ bevor die VO (EU) 2022/991 einen Rechtsrahmen für die Verarbeitung und

⁵³ 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.

⁵⁴ 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: 12.08.2026).

⁵⁵ Dazu Pfeffer/v. Rodbertus, 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, 2026, S. 93 ff.

⁵⁶ 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.

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 Mitgliedstaaten⁵⁷ und andere EU-Agenturen geregelt: Europol soll danach nicht nur 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.“*

Anfang 2026 ist das Zweite Gesetz zur Änderung des Europol-Gesetzes in Kraft getreten, das die deutsche Rechtslage an die geänderte VO (EU) 2022/991 anpasst.⁵⁸ 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 § 188c LVwG-E künftig auch Europol mit einer automatisierten Datenanalyse beauftragt werden kann.

Am 24. Juni 2026 legte die Europäische Kommission einen Verordnungsvorschlag für die weitere Stärkung des Mandats von Europol vor.⁵⁹ Der Vorschlag zielt insbesondere darauf ab, die Rolle von Europol als Informations-, Operations- sowie Technologie- und Innovationszentrum der EU zu stärken und baut auch die automatisierte Datenanalyse der Agentur weiter aus. Der Europäische Datenbeauftragte kritisiert in seiner Stellungnahme aus August 2026 der derzeitige Vorschlag würde es Europol ermöglichen, „Daten einer großen Anzahl von Personen, bei denen kein Zusammenhang mit einer kriminellen Handlung

⁵⁷ 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 bezüglich der Zusammenarbeit mit Europol sowie die Beziehungen dieser Behörden im Verhältnis zueinander bei der Zusammenarbeit mit Europol regeln soll.

⁵⁸ BGBl. 2026 I Nr. 26 vom 05.02.2026; Gesetzesbegründung siehe Entwurf eines Zweiten Gesetzes zur Änderung des Europol-Gesetzes Drs. BT 21/2373 vom 22.10.2025.

⁵⁹ COM(2026) 580 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52026PC0580> (Zugriff: 24.08.2026).

festgestellt wurde, für einen langen und unbestimmten Zeitraum zu speichern“.⁶⁰ Diese Daten würden dann künftig auch von der automatisierten Datenanalyse der Agentur erfasst.

Dass eine Ermächtigungsgrundlage einer Sicherheitsbehörde eines Mitgliedstaates zur automatisierten Datenanalyse geeignet ist, die Art und Weise der Durchführung einer automatisierten Datenanalyse durch eine europäische 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 § 188c LVwG-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 wurde vom BVerfG ebenso bejaht, wie deren grundsätzliche Geeignetheit und Erforderlichkeit zur vorbeugenden Bekämpfung schwerer Straftaten (dazu bereits unter IV.1.).⁶¹ Verfassungsrechtlich entscheidend ist jedoch die Verhältnismäßigkeit im engeren Sinne. Diese hängt maßgeblich vom Gewicht des Grundrechtseingriffs ab, welches das BVerfG bei der automatisierten Datenanalyse als besonders hoch einstuft.⁶² Der Gesetzgeber kann das Eingriffsgewicht der automatisierten Datenanalyse durch verschiedene normative Stellgrößen steuern (dazu bereits unter IV.1.).

1. Herausfordernde Gesetzestechnik

Die Systematik/der Aufbau der Norm des § 188c LVwG-E und § 188d LVwG-E ist besonders herausfordernd:

Dies ist bereits dem Umfang der Regelungen in § 188c LVwG-E mit ihren 8 Absätzen und den Regelungen zum Verfahren bei der Durchführung der automatisierten Datenanalyse in § 188d LVwG-E mit 7 Absätzen geschuldet. Die Art und Weise der Anordnung der verschiedenen Eingriffsschwellen und deren Ausnahmen sowie die Nennung bzw. der Ausschluss der einbezieharen Datenquellen in § 188c LVwG-E machen die Norm äußerst schwer verständlich und für künftige Anwender nur schwer handhabbar. Nur zum Teil liegt dies an dem berechtigten Anspruch, den komplexen verfassungsrechtlichen Vorgaben, die das BVerfG 2023 formuliert hat, gerecht zu werden. Denn die schwere Handhabbarkeit ist auch dem Umstand geschuldet, dass hier zwei unterschiedliche Maßnahmen in einer Norm geregelt werden, der „IT-gestützter Abgleich“ und die „automatisierte Datenanalyse“. Dass die Anforderungen an den Eingriff für den Anwender nur noch schwer zu erfassen ist, dürfte des Weiteren auch daran liegen, dass § 188c LVwG-E mit seinen Absätzen nach dem Umfang der zu verarbeitenden Daten aufgebaut/angeordnet wurde, statt nach dem Zweck der Eingriffe. Hiervon wird dann wohl zum Teil aber wieder abgewichen, etwa wenn dann doch

⁶⁰ EDPS Opinion 18/2026 on the Proposal for a Regulation on Europol repealing Regulation (EU) 2016/794 https://www.brak.de/fileadmin/05_zur_rechtspolitik/stellungnahmen-pdf/stellungnahmen-deutschland/2026/stellungnahme-der-brak-2026-21.pdf (Zugriff: 24.08.2026).

⁶¹ BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 52, 53.

⁶² BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 59, 64.

Zwecke in § 188c Abs. 7 LVwG-E formuliert werden. Verfahrensvorschriften finden sich teilweise in § 188c LVwG-E, überwiegend aber in § 188d LVwG-E.

2. Eingriffsintensität - Art und Umfang der verarbeitbaren Daten

a) Datenanalyse, beschränkt zunächst auf die in § 188c Abs. 3 Satz 1 LVwG-E genannten Datenbestände der Polizei

§ 188c Abs. 3 Satz 1 LVwG-E betrifft die Datenanalyse zu bestimmten Zwecken, wobei der Umfang der Analyse auf die in § 188c Abs. 3 Satz 1 LVwG-E genannten Datenbestände der Polizei begrenzt ist.

§ 188c Abs. 3 Satz 1 LVwG-E zählt auf, welche der rechtmäßig erhobenen und gespeicherten Daten hierbei in die Analyse einbezogen werden. Wie sich aus der Entwurfsbegründung ergibt, soll die Aufzählung „abschließenden Charakter“ haben und so die Eingriffsvoraussetzungen für eine Datenanalyse mit reduziertem Eingriffsgewicht schaffen.⁶³

Nach näherer Betrachtung der hier aufgezählten Datenquellen trägt die abschließende Aufzählung der polizeilichen Datenquellen jedoch wenig dazu bei, die Eingriffstiefe der Maßnahme abzumildern.

Dies liegt zum einen an der Tatsache, dass bereits die hier genannten Datenquellen wenig „eingegrenzt“ sind (hierzu im Folgenden). Außerdem ist der Umfang der Datenquellen ist gem. § 188c Abs. 5 LVwG-E bereits bei einer nicht näher umschriebenen „Erforderlichkeit im Einzelfall“ händisch sehr umfangreich weiter erweiterbar (siehe dazu bereits 1.a.bb) (9)). Dies führt insgesamt zu einer „Entgrenzung“ der analysierbaren Datenquellen insbesondere auch über die Einbeziehung von nicht näher bezeichneten Datenbeständen von Privaten:

Benannt werden in § 188c Abs. 3 Satz 1 LVwG-E: *„Vorgangs- und Fallbearbeitungssysteme, polizeiliche Auskunfts-, Kommunikations-, Einssatzleit- und Einsatzdokumentationssysteme sowie Aserve und andere Beweismittel.“*

Zunächst ist festzustellen, dass der Gesetzgeber bisher gar nicht regelt, wie Daten aus Vorgangs- und Fallbearbeitungssystemen, polizeiliche Auskunfts-, Kommunikations-, Einssatzleit- und Einsatzdokumentationssystemen sowie Aserve und andere Beweismittel zu erheben und die Datenbestände zu verwalten sind. In der polizeilichen Praxis bestehen damit große Spielräume, was den Datenumfang in diesen Systemen betrifft.⁶⁴

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 einen sonstigen Gegenstand

⁶³ Drs. 20/4284 S. 48.

⁶⁴ Hierauf weist auch die BRAK hin, siehe Stellungnahme Nr. 21 April 2026 zur automatisierten Datenanalyse in den Gesetzesentwürfen der Bundesregierung https://www.brak.de/fileadmin/05_zur_rechtspolitik/stellungnahmen-pdf/stellungnahmen-deutschland/2026/stellungnahme-der-brak-2026-21.pdf (Zugriff: 14.08.2026).

polizeilichen Handels geführt werden. In dem Vorgang werden Anzeigen, Ermittlungsberichte und Vermerke aufgenommen, die nicht nur Daten zu Verdächtigen, Beschuldigten oder sonstigen Anlasspersonen enthalten, sondern etwa auch Daten zu Anzeigeerstatlern, 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 z.B. Anzeigeerstatler, 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 ist und vor allem Beziehungen zwischen Personen, Institutionen, Objekten und Sachen aufzeigen kann und sowohl für präventive als auch repressive Zwecke eingesetzt werden kann.

Polizeiliche Auskunftssysteme sind das elektronische Informationssystem der Polizei (INPOL), der Polizeiliche Informations- und Analyseverbund (PIAV), das Programm "Polizei2020", Europäische Informationssysteme, Internationale Informationssysteme, EPRIS (European Police Records Index System). Auch hier sind sehr umfangreiche Datengruppen enthalten:⁶⁵

- *„Kriminalaktennachweise: Diese beinhalten Informationen über laufende und abgeschlossene Ermittlungsverfahren, insbesondere die Straftatbestände, wegen derer ermittelt wurde, Datum und Art der Einstellungsverfügung, deren Gründe, Angaben zur Anklageerhebung sowie zum Ausgang des Hauptverfahrens.*
- *Personenfahndung: Diese listet in einem Katalog den Anlass und den Zweck der Ausschreibung einer Person zur Fahndung mit dem Ziel auf, fahndungsrelevante Erkenntnisse über Täterinnen oder Täter, Tathergang, Zeuginnen oder Zeugen, Geschädigte etc. zu erlangen. Die Personenfahndung dient u. a. der Festnahme oder Aufenthaltsermittlung von Straftäterinnen oder Straftätern (Strafverfolgung) oder dem Schutz von vermissten Personen (Gefahrenabwehr).*
- *Sachfahndung: Sie dient u. a. der Beweissicherung sowie der Ermittlung von Eigentümern und Besitzern von Sachen, die durch eine Straftat oder auf andere Weise abhandengekommen sind.*
- *Haftdatei: Sie beinhaltet Daten von Personen, die wegen des Verdachts oder des Nachweises einer rechtswidrigen Tat einer richterlich angeordneten Freiheitsentziehung unterliegen.*
- *Erkennungsdienst und DNA-Analyse-Datei: Die Erfassung und Speicherung von biometrischen Merkmalen (insbesondere Fingerabdrücke, Lichtbilder und DNA-Identifizierungsmuster) bildet die Grundlage für die Ermittlung von Täterinnen oder Tätern in Strafverfahren, die Zuordnung von Tatortspuren, das Erkennen von Tatzusammenhängen, aber auch die Identifizierung von hilflosen Personen oder unbekannten Toten. Die aus der DNA-Analyse nach § 81 g StPO oder § 15 a StPO*

⁶⁵ Aufzählung entnommen der Drs. 19/8942 des Niedersächsischen Landtages.

gewonnenen Identifizierungsmuster werden in einer zentralen DNA-Analyse-Datei (DAD) gespeichert.“

U.a. mit der Bundesrechtsanwaltskammer (BRAK) und auch einigen Gerichten ist auf die „praktischen Realitäten“ hinzuweisen: „Trotz staatsanwaltlicher und ermittlungsrichtlicher Kontrolle, käme es in der Praxis in steter Regelmäßigkeit zur (grob) rechtswidrigen Speicherung von Daten Beschuldigter, Zeugen und Unbeteiligter“. Es sei „weit verbreitete Praxis“, vorläufig sichergestellte Datenbestände auszuwerten und zur Akte zu nehmen. Verbreitet sei es auch, Datenträger zu beschlagnahmen, obwohl die Verfahrensrelevanz der Daten noch nicht feststeht. Die rechtswidrige Speicherung von Daten betreffe in der Praxis auch immer wieder Berufsgeheimnisträger.⁶⁶

Ein Ausschluss von Daten, die durch besonders schwere Grundrechtseingriffe erlangt wurden, durch den Einsatz technischer Mittel in Wohnungen oder durch den Zugriff auf informationstechnische Systeme, erfolgt bei der automatisierten Analyse zu den Zwecken gem. § 188c Abs. 3 LVwG-E durch § 188c Abs. 6 Satz 1 LVwG-E.

b) Automatisierte Datenanalyse mit sämtlichen Dateisystemen der Polizei und automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden

§ 188c Abs. 4 LVwG-E erlaubt die automatisierte Datenanalyse mit sämtlichen Dateisystemen der Polizei und automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden. Die ohnehin bereits wenig begrenzten verarbeitbaren Datenquellen für die Analyse nach § 188c Abs. 3 Satz 1 LVwG-E (s.o.) werden hier nochmals erweitert.

Da der Gesetzgeber nicht definiert, was „Dateisysteme der Polizei“ sind, bleibt auch hier unklar, was zu „sämtlichen Dateisystemen“ der Polizei zu zählen ist. Es sind auch Daten aus Funkzellenabfragen, § 188c Abs. 5 S. 2 LVwG-E, TKÜ-Quellen und Online-Durchsuchungen, § 188c Abs. 6 S. 1 LVwG-E, analysierbar. Die zeitliche Begrenzung der Dauer einer Profilbildung findet hier keine Anwendung, § 188c Abs. 7 S. 2 LVwG-E.

Die Eingriffstiefe mildernde Einschränkungen sind vorgesehen: Die Einbeziehung von Daten, die durch besonders schwere Grundrechtseingriffe erlangt wurden, nämlich durch den Einsatz technischer Mittel in Wohnungen, ist nur erlaubt zur Abwehr einer dringenden Gefahr, also einer zeitlich qualifizierten Gefahr, § 188c Abs. 4 Satz 2 LVwG-E. Außerdem darf dies dann nur zum Schutz besonders hochrangiger Rechtsgüter i.S.v. § 100e Abs. 6 Ziff. 2 StPO erfolgen.

Die Eingriffsintensität hätte durch eine Beschränkung der Herkunft der Daten auf solche, die ursprünglich durch inländische Polizeibehörden erhoben worden sind, vorgenommen werden können. Dies ist in § 188c Abs. 4 LVwG-E aber nicht erfolgt. So 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

⁶⁶ BRAK, Stellungnahme Nr. 21 April 2026 zur automatisierten Datenanalyse in den Gesetzesentwürfen der Bundesregierung S. 16 mit Verweis auf BVerfG, Beschl. v. 17.11.2022, 2 BvR 827/21 und LG Hamburg, Beschl. v. 5.6.2025 . 616 Qs 14/25, Rn. 25 https://www.brak.de/fileadmin/05_zur_rechtspolitik/stellungnahmen-pdf/stellungnahmen-deutschland/2026/stellungnahme-der-brak-2026-21.pdf (Zugriff: 14.08.2026).

polizeilichen Datenbeständen befinden, in eine Analyseplattform nach § 188c LVwG-E einbezogen werden.

c) Weitere Grundsätze

aa) Ausschluss einer „Superdatenbank“, Zweckbindung

Ein ganz neuer Eingriff von besonderer Eingriffsintensität bestünde im Anlegen einer neuen vorsorglichen „Superdatenbank“. Mangels verfassungsrechtlicher Rechtfertigung wäre dies verfassungswidrig.⁶⁷ Zu begrüßen ist es daher, dass § 188c Abs. 2 LVwG-E zur Vermeidung der Erstellung einer dauerhaften „Superdatenbank“ regelt, dass die Weiterverarbeitung der Daten nur zum Zweck der Analyse erfolgen darf. Die bereits zusammengeführten Daten dürfen gem. § 188c Abs. 2 LVwG-E im jeweiligen Einzelfall nur in dem Maße verarbeitet werden, wie das für den jeweiligen Analysezweck erforderlich ist. Der Inhalt der so zusammengeführten Dateien darf nur in dem Umfang verwendet werden, wie es die Zweckbindung vorsieht, dies stellt § 188c Abs. 2 Satz 2 LVwG-E klar. Diese Vorgaben sollen gem. § 188c Abs. 2 LVwG-E für sämtliche in § 188c Abs. 3 und 4 LVwG-E genannten Zwecke der automatisierten Datenanalyse gelten.

bb) Ausschluss biometrischer Daten

Als eingriffsbegrenzend zu begrüßen ist die Regelung, wonach weder bei dem IT-gestützten Datenabgleich, noch bei der automatisierten Datenanalyse, unabhängig von deren jeweiligen Eingriffszweck, biometrische Daten verarbeitet werden dürfen (§ 188c Abs. 6 Satz 2 Ziff. 1 LVwG-E).

cc) Ausschluss selbstlernender Systeme

Eingriffsmildernd wirkt auch der generelle Ausschluss des Einsatzes selbstlernender Systeme gem. § 188c Abs. 6 Satz 2 Ziff. 2 LVwG-E.

Laut BVerfG verbietet das Grundgesetz lernende Systeme zwar nicht generell.⁶⁸ 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 nicht zwischen Echtzeitlernmodellen und fixierten Modellen unterschieden hat. Es könne der Eindruck entstehen, das BVerfG habe nur zu Echtzeitlernmodellen urteilen wollen.⁶⁹

Unabhängig davon war das BVerfG jedenfalls sehr klar bei der Forderung, dass der Gesetzgeber beim Einsatz einer automatisierten Datenanalyse im Vorfeld einer

⁶⁷ Botta, Verfassungswidrige Superdatenbank: Die dauerhafte Zusammenführung polizeilicher Datenbestände als eigenständiger Grundrechtseingriff, VerfBlog, 2026/9/01, <https://verfassungsblog.de/palantir-superdatenbank/> (Zugriff 01.09.2026),

⁶⁸ BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 100.

⁶⁹ 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.

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.“⁷⁰

dd) Kein unmittelbarer automatisierter Abgleich von personenbezogenen Daten aus Internetdiensten

Eingriffsmildernd wirkt hier zudem der ausdrückliche Ausschluss einer direkten Anbindung der Analyseplattform an Internetdienste gem. § 188c Abs. 6 Satz 2 Ziff. 3 LVwG-E.⁷¹

Wenn dies im Einzelfall erforderlich ist, dann können gem. § 188c Abs. 5 Satz 1 LVwG-E allerdings gesondert gespeicherte Datensätze aus Internetquellen (händisch) einbezogen werden.

ee) Verbot automatisierter Entscheidungsfindung

Vor dem Hintergrund der Gewährleistung der Menschenwürde (Art. 1 Abs. 1 GG) und des Demokratieprinzips (Art. 20 Abs. 1, 2 GG) wäre es empfehlenswert, dass die Landesregierung das Letztentscheidungsgebot hier ausdrücklich verankert.⁷² Wegen der Grundrechtsbindung gem. Art. 1 Abs. 3 GG und des Rechtsstaatsprinzips 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.⁷³

ff) Begrenzung der Suchkriterien

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.⁷⁴ Es ist daher zu begrüßen, wenn der Gesetzgeber hier ausdrücklich regelt, dass nur solche Suchkriterien verwendet werden dürfen, die auf den Anlass zurückgeführt werden können, § 188d Abs. 2 Satz 1 LVwG-E.

gg) Ausschluss diskriminierender Algorithmen

Nach § 188d Abs. 3 Satz 1 LVwG-E muss die Nachvollziehbarkeit des verwendeten automatisierten Verfahrens sichergestellt werden. Gem. § 188d Abs. 3 Satz 2 LVwG-E dürfen Algorithmen, deren Regeln gruppenbezogenen Merkmalen iSd Art. 3 Abs. 3 GG folgen, ohne dass dies durch den Zweck der Datenanalyse gerechtfertigt ist, nicht verwendet werden. Diese Regelung ist begrüßenswert. Offen läßt der Gesetzgeber jedoch, wie diskriminierende Algorithmen verhindert werden und die Nachvollziehbarkeit sichergestellt werden sollen.

⁷⁰ BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 120f.

⁷¹ BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 88.

⁷² Martini/Botta DÖV 2025, 1033, 1042 zu § 47 Abs. 1 Satz 3 PolG BW.

⁷³ Martini/Botta DÖV 2025, 1033, 1042.

⁷⁴ BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 164 ff.

hh) Einbeziehung von weiteren Datenquellen im Einzelfall (händisch)

§ 188c Abs. 5 Satz 1 LVwG-E erlaubt die Einbeziehung von weiteren Datenquellen im Einzelfall, wenn dies zur Aufklärung des Sachverhalts im Einzelfall erforderlich ist. Die genannten Datenquellen sollen dann „händisch“ bezogen werden. Laut der Rechtsprechung des BVerfG kann es zur Reduktion der Menge verarbeitbarer Daten beitragen,⁷⁵ wenn vorgegeben wird, dass Dateien nicht automatisiert einbezogen werden, sondern für jeden Analyse- oder Auswertungsvorgang händisch hinzugezogen werden müssen. Da der Gesetzgeber hier aber nicht selbst regelt, wann die Hinzuziehung weiterer Datenquellen „erforderlich“ ist, bleibt die Einschätzung schließlich der Exekutive überlassen. Es erscheint fraglich, ob sich diese Regelung in der praktischen Umsetzung tatsächlich als eingriffsmindernd erweisen wird.

Zu den im Einzelfall händisch einzubeziehenden Datenquellen:

➤ **Gesondert geführte staatliche Register**

Hinzugezogen werden dürfen dann auch Datensätze aus gezielten Abfragen gesondert geführter staatlicher Register. Solche Register können Melde-, Waffenregister oder das zentrale Verkehrsinformationssystem (ZEVIS) sein.

➤ **Einzelne gesondert gespeicherte Datensätze aus Internetquellen**

Außerdem dürfen dann auch einzelne gesondert gespeicherte Datensätze aus Internetquellen einbezogen werden, eine direkte Anbindung ist nicht vorgesehen. Auch die Einbeziehung von allen in einer Funkzelle anfallenden Verkehrsdaten ist in einem solchen Einzelfall möglich, § 188 Abs. 5 Satz 2 LVwG-E bei einer Analyse nach § 188c Abs. 3 LVwG-E.

➤ **Polizeilich nutzbare Auskunft- und Informationssysteme**

Weiterhin dürfen auch „polizeilich nutzbare Auskunft- und Informationssysteme“ hinzugezogen werden. Der Gesetzgeber hat aber nicht geregelt, was ein „polizeilich nutzbares Auskunft- und Informationssystem“ darstellt.

➤ **Von Dritten geführte Datenbestände**

Schließlich sollen „von Dritten geführte Datenbestände“ händisch einbezogen werden dürfen. Dies ist verfassungsrechtlich außerordentlich problematisch: Da hier keine Anforderungen an die Herkunft der Daten vorgesehen sind, könnte sich dies auf jede Art von personenbezogenen Daten erstrecken (einschließlich personenbezogener Daten, die ursprünglich zu kommerziellen Zwecken erhoben wurden). Bei kommerziell erworbenen Daten ist häufig nicht gewährleistet, dass diese rechtmäßig erhoben wurden. Die Polizei würde auf diese Weise in die Lage versetzt, potenziell große Mengen personenbezogener Daten zu verarbeiten, die direkt von privaten Stellen übermittelt wurden, einschließlich Daten, die sich auf völlig Unbeteiligte beziehen, die in keinen Zusammenhang mit einer

⁷⁵ BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 88.

Gefahr oder Straftat stehen.⁷⁶ So könnte die Polizei z.B. mit Standortdaten aus der Werbeindustrie ähnliche Ergebnisse erzielen, wie mit Funkzellenabfragen & IMSI-Catchern, letztere unterliegen jedoch einem Richtervorbehalt.

ii) Bildung von Verhaltens- und Bewegungsprofilen

§ 188c Abs. 7 LVwG-E ermöglicht das Erstellen eines Bewegungs- oder Verhaltensprofils mittels automatisierter Datenanalyse. Laut BVerfG ist es als besonders intensiver Grundrechtseingriff zu werten,⁷⁷ „wenn sich das Verhalten einer Person, deren Gewohnheiten oder deren Lebensgestaltung räumlich und über längere Zeit hinweg nachvollziehen lassen, wenn also ein Bewegungs- oder Verhaltensprofil einer Person oder ein umfassenderes Persönlichkeitsbild entstehen kann“.

Verboten nach der KI-VO ist 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). Dieses Verbot erfasst lediglich ein Predictive Policing, welches sich ausschließlich auf ein personenbezogenes Profiling 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 § 188c LVwG-E nicht ab, dies stellt § 188c Abs. 7 Satz 3 LVwG-E klar.

Eine zeitliche Beschränkung enthält § 188c Abs. 7 Satz 2 LVwG-E nur für eine Datenanalyse nach § 188c Abs. 3 LVwG-E. Danach darf der Zeitraum höchstens eine Woche umfassen.

3. Zwischenergebnis

Mit §§ 188c, 188d LVwG-E sollte eine nach dem Eingriffszweck abgestufte Einbeziehung von Datenquellen geregelt werden. Insgesamt ist das Eingriffsgewicht wegen des wenig eingegrenzten Umfangs der Daten, sowohl bei § 188c Abs. 3 LVwG-E, als auch bei § 188c Abs. 4 LVwG-E auch trotz einiger eingriffsreduzierender Regelungen als hoch einzustufen.

Der Ansatz mit § 188c Abs. 5 Satz 1 LVwG-E, wonach zahlreiche weitere Datenquellen nur im Einzelfall nach Erforderlichkeit händisch hinzugezogen werden dürfen, wirkt grundsätzlich eingriffsmildernd. Der Gesetzgeber regelt aber selbst nicht, wann eine solche „Erforderlichkeit“ anzunehmen ist. Einige der so hinzuziehbaren Datenquellen, insbesondere die Einbeziehung der Daten Dritter, wie sie derzeit geregelt ist, erscheint verfassungsrechtlich nicht vertretbar. Regelungen zu den zugelassenen Datenarten (vgl. etwa § 3 Abs. 1 ATDG oder § 29 Abs. 2a S. 3 GwG) fehlen.

Bereits die in § 188c Abs. 3 LVwG-E genannten Datenquellen (Stufe 1) sind bei genauerer Betrachtung wegen unbestimmter Tatbestände (Falldaten, Vorgangsdaten) wenig begrenzt.

⁷⁶ So auch der Europäische Datenschutzbeauftragte EDPS Opinion 18/2026 on the Proposal for a Regulation on Euro-pol repealing Regulation (EU) 2016/794 https://www.edps.europa.eu/data-protection/our-work/publications/opinions/2026-08-11-edps-opinion-182026-regulation-europol-repealing-regulation-eu-2016794_en (Zugriff: 24.08.2026).

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

Dies setzt sich in § 188c Abs. 4 LVwG-E fort (Stufe 2) und wurde so auch vom Gesetzgeber selbst eingeschätzt.

4. Verfahrensanforderungen zum Zwecke der Nachvollziehbarkeit, Transparenz und behördlichen Kontrolle

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.⁷⁸ 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.⁷⁹ Die wesentlichen Leitplanken für Verfahren zur Durchführung der automatisierten Datenanalyse sind durch die Legislative selbst festzulegen.

a) Anordnungsbefugnis, Richtervorbehalt § 188c Abs. 8 LVwG-E

Der Gesetzesentwurf regelt näheres zur Anordnungsbefugnis:

§ 188c Abs. 8 Satz 2 Ziff. 1 LVwG-E regelt für die automatisierte Datenanalyse, die nach Abs. 3, (zunächst) auf die dort genannten Quellen beschränkt ist, dass sie von der Polizei nach Maßgabe von § 186 Abs. 2 LVwG angeordnet werden muss. Danach erfolgt die Anordnung „durch die Leiterin oder den Leiter des Landespolizeiamtes, des Landeskriminalamtes, einer Polizeidirektion oder durch von ihr oder ihm besonders beauftragte Personen des Polizeivollzugsdienstes, bei Gefahr im Verzug durch jede Polizeivollzugsbeamtin oder jeden Polizeivollzugsbeamten.“

Als Voraussetzung (jedoch nur) für die erweiterte automatisierte Datenanalyse nach § 188c Abs. 4 LVwG-E sieht § 188c Abs. 8 Satz 2 Ziff. 2 LVwG-E eine richterliche Anordnung nach Maßgabe von § 186 Abs. 1 LVwG vor. Es wird empfohlen, die richterliche Anordnung auch auf Maßnahmen nach Abs. 3 zu erstrecken.

Für das Erstellen eines Bewegungs- oder Verhaltensprofils nach § 188c Abs. 7 LVwG-E regelt § 188 Abs. 8 Satz 3 LVwG-E, dass dies in der richterlichen Anordnung ausdrücklich zugelassen werden muss. Zu weiteren Anforderungen wird hier auf die Regelungen in § 186 Abs. 3 Satz 1, 2, 4, 5 und Abs. 4 sowie Abs. 5 LVwG verwiesen.

b) Kennzeichnungspflicht, § 188d Abs. 1 LVwG-E

Voraussetzung einer begrenzenden Wirkung von Vorgaben zu Art und Umfang der Daten ist, dass die betroffenen personenbezogenen Daten gekennzeichnet werden.⁸⁰ Der Gesetzgeber trifft hierzu selbst in § 188d Abs. 1 LVwG-E entsprechende Regelungen.

c) Qualifikation, Zugangskontrolle, Protokollierung § 188d Abs. 4 LVwG-E

§ 188d Abs. 4 Satz 1 LVwG-E regelt, dass der Zugang zu den Anwendungen nach § 188c LVwG auf „bestimmte diesbezüglich qualifizierte Beschäftigte der Polizei“ beschränkt ist. Wie die Beschäftigten auszuwählen und zu qualifizieren sind, d.h. das „wie“, wird nicht geregelt.

⁷⁸ BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 109; Kugelman/Buchmann, GSZ 2024, S. 1, 9f.

⁷⁹ Kugelman/Buchmann, GSZ 2024, S. 1, 9.

⁸⁰ 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.

Der Einsatz automatisierter Datenanalysesysteme (Hochrisiko-KI) erfordert das Verständnis für deren Fehleranfälligkeit, für Diskriminierungsrisiken von Algorithmen und auch für das Phänomen der "Halluzinationen".

Gem. Art. 4 KI-VO (KI-Kompetenz) müssen Anbieter und Betreiber von KI-Systemen Maßnahmen ergreifen,

“um die Entwicklung der KI-Kompetenz ihres Personals und anderer Personen zu unterstützen, die in ihrem Auftrag mit dem Betrieb und der Nutzung von KI-Systemen befasst sind, wobei ihre technischen Kenntnisse, ihre Erfahrung, ihre Aus- und Fortbildung 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. Diese Verpflichtung verpflichtet Anbieter oder Betreiber nicht, für irgendeine Person ein bestimmtes Niveau an KI-Kompetenz zu garantieren.“

Es wäre daher zu empfehlen, vergleichbar dem § 9b Abs. 6 S. 1 BKAG-E-Polizeiarbeit sowie die dessen Parallelvorschrift § 39b Abs. 6 S. 1 BKAG-E-Terrorismus, für die automatisierte Datenanalyse eine Schulungspflicht für die einzusetzenden Beschäftigten ausdrücklich zu regeln.⁸¹

Weitere technische und organisatorische Maßnahmen, die sicherstellen sollen, dass die Zugriffsmöglichkeiten des eingesetzten Personals auf die zur Verfügung stehenden personenbezogenen Daten auf das erforderliche Maß beschränkt werden, enthält § 188d Abs. 4 Satz 2 LVwG-E, wonach neben der Protokollierungspflicht geregelt wird, dass die Beschäftigten, die die Maßnahme durchführen, erfasst werden.

d) Verweis auf Betreiberpflichten nach Art. 26 KI-VO, § 188d Abs. 4 Satz 3 LVwG-E.

Auch wenn Art. 26 KI-VO (Betreiberpflichten) als EU-Verordnung direkt verbindlich ist, ist ein Verweis aus Gründen der besseren Transparenz hier zu begrüßen.

e) Datenvorhaltung nach Zusammenführung (Superdatenbank), § 188d Abs. 5 LVwG-E

§ 188d Abs. 5 LVwG-E enthält weitere Regelungen zur Verhinderung einer dauerhaften Superdatenbank nach der Zusammenführung von Daten.

f) Information des Betroffenen, § 188d Abs. 6 Satz 1 LVwG-E

Die Verankerung einer Informationspflicht gegenüber der von der Maßnahme betroffenen Person dient dem effektiven Rechtsschutz iSv Art. 19 Abs. 4 GG. Denn die Kenntnis von der automatisierten Datenanalyse ist hierfür Voraussetzung. Ein solcher möglicher Rechtsschutz dient auch nicht allein der Feststellung der Rechtmäßigkeit/Rechtswidrigkeit der automatisierten Datenanalyse (retrospektiv), sondern kann ggf. auch anschließende grundrechtsintensive Folgemaßnahmen verhindern.

⁸¹ Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit BT-Drs. 21/6231, 26.05.2026, <https://dserver.bundestag.de/btd/21/061/2106132.pdf> sowie mit dem Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse zur Abwehr von Gefahren des internationalen Terrorismus, BT-Drs. 21/6131, 26.05.2026, <https://dserver.bundestag.de/btd/21/061/2106131.pdf> (Zugriff: 25.08.2026); als unzureichend kritisiert von Rohrbach, Wegducken vor den Fragen des digitalen Zeitalters: Die automatisierte Datenanalyse braucht menschenrechtliche Grenzen, weil menschliche Grenzen obsolet werden, VerfBlog, 2026/8/31, <https://verfassungsblog.de/palantir-diskriminierung-menschenrechte/>, DOI: 10.59704/bbb8810cdeefb3d (Zugriff: 01.09.2026).

g) Delegation von technisch-organisatorischen Einzelheiten, § 188d Abs. 7 LVwG-E

Der Gesetzgeber darf hier gem. BVerfG von 2023 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 entsprechen.⁸² Der Gesetzesentwurf benennt hier die näher zu regelnden Materien in § 188d Abs. 7 Ziff. 1-7 LVwG-E.

Der Gesetzesentwurf sieht dafür aber eine (veröffentlichungsbedürftige) Verwaltungsvorschrift vor. Die Delegation erfolgt auch an das Ministerium, welches für Inneres zuständig ist und nicht in das Amt Polizei selbst.

Überträgt der Gesetzgeber der Verwaltung Näheres zu regeln, ist eine Verordnungsermächtigung jedoch vorzugswürdig.⁸³ Denn hierbei handelt es sich um ein Gesetz mit Außenwirkung.

5. 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 (s.o.).

a) Zu § 188c Abs. 3 Ziff. 2 LVwG-E

§ 188c Abs. 3 Satz 1 Ziff. 2 LVwG-E erlaubt die automatisierte Datenanalyse bereits für die vorbeugende Bekämpfung von Straftaten. Nach der Rechtsprechung des BVerfG ist hierbei zur Wahrung der Verhältnismäßigkeit die Eingriffsintensität der Maßnahme reduzieren.⁸⁴

Gemäß § 188c Abs. 3 Satz 2 LVwG-E ist eine automatisierte Datenanalyse (nur) für hochrangige Rechtsgüter erlaubt, Ziff. 1-3.

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 Eigengewicht des Eingriffs mindert oder aber die Maßnahme auf hinreichend konkretisierte Gefahren begrenzt.⁸⁵ Andernfalls müsste hier eine Eingriffsschwelle greifen, die dem repressiven Instrumentarium entspricht – richterlicher Vorbehalt, Benachrichtigungspflichten und strenge Dokumentation eingeschlossen.

Der Gesetzgeber sieht in § 188c Abs. 3 LVwG-E konkretisierte Gefahren als Eingriffsschwelle vor. Für den äußerst grundrechtsintensiven Fall sieht § 188c Abs. 8 Satz 2 Ziff. 2 LVwG-E eine richterliche Anordnung nach Maßgabe von § 186 Abs. 1 LVwG vor.

⁸² BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 110, 112.

⁸³ BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 113.

⁸⁴ BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 112.

⁸⁵ BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 47 ff.

b) Zu § 188c Abs. 4 LVwG-E

Aufgrund des hohen Eingriffsgewichts soll die automatisierte Datenanalyse nur zur Abwehr konkreter Gefahren für besonders gewichtige Rechtsgüter nach § 188c Abs. 3 Satz 1 Ziff. 1 LVwG-E zulässig sein. Es spricht viel dafür, hier auch die sexuelle Selbstbestimmung als ein „besonders gewichtiges Rechtsgut“ einzustufen. So spricht das BVerfG bei Straftaten gegen die sexuelle Selbstbestimmung von „erheblichen Straftaten“.⁸⁶

VII. Fazit

Die Landesregierung schlägt mit ihrem Gesetzesentwurf eine Modernisierung des Schleswig-Holsteinischen Polizeirechts vor. Soweit hier betrachtet (§§ 188c, 188d LVwG-E), 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 (§§ 188c, 188d LVwG-E) noch Nachbesserungsbedarf. Ich empfehle den Entwurf insoweit entsprechend anzupassen.

gez.

Prof. Dr. iur. Kristin Pfeffer

⁸⁶ BVerfG, Beschluss v. 1. Dezember 2020 - 2 BvR 916/11; 2 BvR 636/12 Rn. 121.