Deutsches Forschungsinstitut
für öffentliche Verwaltung

FÖV / Postfach 14 09 / 67324 Speyer

An den Ausschuss für Inneres, Sicherheit und
Ordnung des Abgeordnetenhauses von Berlin

Dr. Jonas Botta
Forschungsreferent
botta@foev-speyer.de

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

Sehr geehrte Damen und Herren Abgeordnete,

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

Mit freundlichen Grüßen

Jonas Botta

DR. JONAS BOTTA*

Gesetz zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin

(AGH-Drs. 19/2553)

* **Dr. Jonas Botta** vertritt derzeit die Juniorprofessur für Öffentliches Recht mit Schwerpunkt Datenschutzrecht und Recht der Digitalisierung an der FernUniversität in Hagen und ist zugleich Forschungsreferent am Deutschen Forschungsinstitut für öffentliche Verwaltung (FÖV Speyer). Seit 2019 lehrt er außerdem Grund- und Menschenrechte sowie Öffentliches Dienstrecht im Polizeistudium an der HWR Berlin. Er fungiert regelmäßig als parlamentarischer Sachverständiger auf Bundes- und Landesebene zu Fragen des Verfassungs-, Europa- Polizei- und Digitalrechts.

A. Überblick

Die Fraktionen von CDU und SPD haben zu Recht die Notwendigkeit erkannt, das ASOG an die Herausforderungen des 21. Jahrhunderts anzupassen. Damit dieses Ziel erreicht werden kann, sind nicht nur rechtliche und technische Neuerungen erforderlich, sondern auch eine sorgfältige **Beachtung des Verfassungs- und Unionsrechts**. Der gegenwärtige Gesetzentwurf erfüllt diese Anforderung bislang noch nicht ausreichend.

Die nachfolgende Stellungnahme konzentriert sich – neben einer Klarstellung zu den Kompetenzen des **Polizeibeauftragten (§ 24c Abs. 7 Nr. 3 ASOG-E)** – auf zwei Regelungsvorschläge, die von besonderer Brisanz sind: die Ermächtigungsgrundlagen zum **Training bzw. zur Testung von KI-Systemen (§ 42d ASOG-E)** und zur **automatisierten Datenanalyse (§ 47a ASOG-E)**. Beide Befugnisse sind nicht nur äußerst grundrechtssensibel, sie betreffen auch eine große Personenanzahl – sowohl aus Berlin als auch aus dem gesamten Bundesgebiet (und darüber hinaus). Es ist daher positiv hervorzuheben, dass sich die Fraktionen von CDU und SPD ersichtlich darum bemüht haben, bei der Erarbeitung der Normen die einschlägige Rechtsprechung des BVerfG möglichst umfassend zu berücksichtigen. Gleichwohl verstoßen beide Regelungsvorschläge derzeit noch gegen höherrangiges Recht und sind daher vor ihrer Verabschiedung zu überarbeiten.

Sollte das Abgeordnetenhaus nicht die erforderlichen Korrekturen vornehmen, schwebte über der angestrebten Modernisierung der Gefahrenabwehr dauerhaft das Damoklesschwert der **Verfassungswidrigkeit**. Dann fiele es höchstwahrscheinlich dem BVerfG zu,[1] nachträglich für einen verfassungsgemäßen Zustand zu sorgen, was nicht nur die Polizeiarbeit erschwerte, da bereits etablierte Verfahren geändert werden müssten, sondern vor allem auch das gesellschaftliche **Vertrauen in die Polizei und den Rechtsstaat** insgesamt beschädigte.

[1] Gegen den reformierten § 25a HSOG (Automatisierte Anwendung zur Datenanalyse) wurde bereits Verfassungsbeschwerde erhoben. Online abrufbar unter: https://freiheitsrechte.org/uploads/documents/Freiheit-im-digitalen-Zeitalter/Polizeigesetz -Hessen/Verfassungsbeschwerdeschrift-HSOG.pdf.

Es ist zudem entschieden **als Fehlentwicklung zu kritisieren, wenn die Legislative die Fortschreibung des Sicherheitsrechts immer mehr dem BVerfG überlässt** und sich überwiegend darauf beschränkt, die von Karlsruhe aufgezeigten Grenzen (nachträglich) in den Normtext zu übernehmen. Damit steht der Berliner Gesetzgeber freilich vor Herausforderungen, die auch schon in anderen Ländern und im Bund aufgetreten sind oder noch auftreten werden. Es zeigt sich (nicht nur) vor diesem Hintergrund, dass insbesondere im Bereich der digitalen Gefahrenabwehr ein **einheitliches, wissenschaftlich fundiertes Musterpolizeigesetz**[2] fehlt. Perspektivisch sollte das Land Berlin daher aktiv auf die Schaffung eines derartigen Regelungsentwurfs durch eine **Sachverständigenkommission aus Wissenschaft und Praxis** hinwirken.

B. Bild- und Tonaufnahmen und -aufzeichnungen zur Eigensicherung und zum Schutz von Dritten (§ 24c ASOG-E)

Die Rechtsgrundlage des § 24c ASOG-E erlaubt es insbesondere den Einsatzkräften der Polizei, der Feuerwehr und des Rettungsdienstes, Bodycams und Dashcams zu ihrem Schutz oder zum Schutz von Dritten zu verwenden. Die dabei aufgezeichneten Bild- und Tonaufnahmen kann u.a. der Berliner **Polizeibeauftragte zur Sachverhaltsaufklärung** verwenden (§ 24c Abs. 7 S. 4 Nr. 3 ASOG-E). Das kann in vielen Fällen entscheidend dafür sein, dass der Beauftragte seinen gesetzlichen Auftrag als unabhängige Ombudsperson erfüllen kann.[3]

In der Praxis läuft diese Vorschrift jedoch weitgehend leer. Wie der **wissenschaftliche Evaluationsbericht des Integrated Research Institute Law & Society** zeigt, vertreten die Polizei Berlin und die Berliner Staatsanwaltschaft die Auffassung, dass Bodycam-Aufnahmen nach Einleitung eines Ermittlungsverfahrens ausschließlich diesem Verfahren zugeordnet sind. Das bedeutet: Nicht mehr die Polizei, sondern die Staatsanwaltschaft müsste dann über ein

[2] Dazu z.B. Aden/Fährmann, Polizeirecht vereinheitlichen? Kriterien für Muster-Polizeigesetze aus rechtsstaatlicher und bürgerrechtlicher Perspektive, 2018.

[3] Weiterführend dazu z.B. Botta, JZ 2022, 664 (667 f.).

Auskunftsersuchen entscheiden (§ 480 Abs. 1 Satz 1 StPO) – unter Anwendung der sehr restriktiven Auskunftsregelungen der Strafprozessordnung (§ 474 Abs. 2 StPO).[4]

Der Evaluationsbericht zeigt jedoch zugleich überzeugend auf, dass § 24c Abs. 7 Satz 4 Nr. 3 ASOG-E auch dann weiter gelten muss, wenn bereits ein Ermittlungsverfahren läuft. Diese Auslegung ist nicht nur notwendig, um die im Gesetz angelegte **Kontroll- und Transparenzfunktion** zu gewährleisten. Sie entspricht auch der **technischen Realität**: Die Originalaufnahmen werden weiterhin zentral bei der Polizei gespeichert, auch wenn eine Kopie an die Staatsanwaltschaft übermittelt wurde. Die Dateien können technisch problemlos für unterschiedliche Zwecke verwendet und mehreren Verfahren zugeordnet werden.

Um zukünftige Rechtsstreitigkeiten zu vermeiden, sollte der Gesetzgeber **in der Begründung zum Gesetzentwurf klarstellen, dass § 24c Abs. 7 S. 4 Nr. 1 ASOG-E keine Sperrwirkung gegenüber § 24c Abs. 7 S. 4 Nr. 3** entfaltet.

C. Training und Testung von KI-Systemen (§ 42d ASOG-E)

Mit § 42d ASOG-E soll ein **datenschutzrechtlicher Erlaubnistatbestand** für die Weiterverarbeitung personenbezogener Daten im Zusammenhang mit dem Training und der Erprobung von KI-Systemen geschaffen werden. Der Entwurf orientiert sich dabei erkennbar an **§ 37a Hamburgisches Gesetz über die Datenverarbeitung der Polizei** (HmbPolDVG), das derzeit insbesondere den Einsatz von Videoaufnahmen aus dem öffentlichen Raum zum KI-Training ermöglichen soll.[5]

Die datenschutzrechtliche Zulässigkeit des Berliner Gesetzentwurfs beurteilt sich in erster Linie nach dem unionsrechtlichen Datenschutzrahmen, insbesondere nach der Richtlinie (EU) 2016/680 (JI-RL),

---

[4] Margies/Hensel/von Steinsdorff/Kaiser/Blokland, Bodycams bei der Polizei Berlin und der Berliner Feuerwehr, Evaluation der Anwendung und Auswirkungen des § 24c Allgemeines Sicherheits- und Ordnungsgesetz, https://www.parlament-berlin.de/ados/19/InnSichO/vorgang/iso19-0207-Abschlussbericht%20Evaluation%20Bodycams.pdf.

[5] Siehe dazu z.B. einen NDR-Bericht v. 31.7.2025, https://www.ndr.de/nachrichten/hamburg/polizei-hamburg-will-ki-mit-videos-von-passantentrainieren,kameraueberwachung-102.html.

die unter anderem durch das Berliner Datenschutzgesetz (BlnDSG) in nationales Recht umgesetzt wurde. Dass der Unionsgesetzgeber im Bereich der nationalen Sicherheit über keine Regelungskompetenz verfügt (Art. 4 Abs. 2 EUV), steht dem nicht entgegen. Denn nach der Rechtsprechung des EuGH ist **zwischen nationaler und öffentlicher Sicherheit zu unterscheiden**:[6] Nationale Sicherheit erfasst ausschließlich den Schutz des Staates selbst, etwa vor terroristischen Bedrohungen, und fällt daher nicht unter den Anwendungsbereich der JI-RL. Maßnahmen wie das polizeiliche KI-Training betreffen hingegen die öffentliche Sicherheit und unterliegen damit dem Anwendungsbereich des Unionsrechts.

I. Wahrung des Zweckbindungsgrundsatzes (Art. 4 Abs. 1 lit. b JI-RL)

Der Erlaubnistatbestand steht im Spannungsverhältnis zum datenschutzrechtlichen Zweckbindungsgrundsatz (Art. 8 Abs. 2 S. 1 Grundrechtecharta der EU [GRCh] bzw. Art. 4 Abs. 1 lit. b JI-RL). Danach müssen personenbezogene Daten grundsätzlich für **festgelegte, eindeutige und legitime Zwecke** erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. § 42d ASOG-E erlaubt aber eine Weiterverarbeitung mit geändertem Zweck (Testung und Training von KI-Systemen, die der Erfüllung der Aufgaben von Polizei bzw. Feuerwehr dienen).

II. Zulässigkeit einer Zweckänderung (Art. 4 Abs. 2 JI-RL)

Unter der JI-RL ist eine Zweckänderung indes **nicht generell ausgeschlossen**. Vielmehr sieht Art. 4 Abs. 2 JI-RL vor, dass eine Weiterverarbeitung personenbezogener Daten zulässig ist, soweit der Verantwortliche nach dem Unionsrecht oder dem Recht der Mitgliedstaaten befugt ist, solche personenbezogenen Daten für diesen anderen Zweck zu verarbeiten, und die Verarbeitung für diesen anderen Zweck nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich und verhältnismäßig ist.

[6] EuGH, CR 2008, 381 (382); Botta, CR 2020, 82 (85); Pilniok, DÖV 2024, 581 (584).

Das Kriterium der Erforderlichkeit ist dabei nicht gesondert zu prüfen, sondern Bestandteil der Verhältnismäßigkeitsprüfung, wie sich aus der Rechtsprechung des EuGH ergibt. Danach müssen sich Ausnahmen und Einschränkungen in Bezug auf den Schutz personenbezogener Daten auf das **absolut Notwendige** beschränken, um dem Erfordernis der Verhältnismäßigkeit zu genügen, was voraussetzt, dass die gesetzliche Verarbeitungsgrundlage hinreichend bestimmt und verfahrensrechtlich abgesichert ist.[7]

Nach dem aktuellen Entwurfsstand ist der in § 42d ASOG-E vorgesehene Erlaubnistatbestand **unverhältnismäßig**.

Besonders kritisch ist die Regelung, wonach bereits dann auf eine Anonymisierung oder Pseudonymisierung verzichtet werden darf, wenn diese mit **unverhältnismäßigem Aufwand** verbunden wäre. Dies stellt eine erhebliche Schwächung des technischen Datenschutzes dar – umso schwerwiegender, als die Norm auch die Verarbeitung personenbezogener Daten zum Training oder zur Testung von **Hochrisiko-KI-Systemen** erlaubt. § 42d ASOG-E verweist pauschal auf den KI-Begriff des Art. 3 Nr. 1 Verordnung über künstliche Intelligenz (KI-VO), ohne eine risikobezogene Einschränkung vorzunehmen, etwa auf weniger eingriffsintensive Systeme.

Problematisch ist außerdem, dass die Vorschrift die **Übermittlung personenbezogener Daten an Auftragsverarbeiter und sogar an Dritte** erlaubt, ohne gleichzeitig ausreichende technische und organisatorische Schutzmaßnahmen vorzuschreiben. Dadurch entstehen erhebliche Risiken für die Datensicherheit. Statt eines vorschnellen IT-Outsourcings sollte sichergestellt werden, dass die Datenverarbeitung grundsätzlich in der Verantwortung der Berliner Behörden verbleibt und externe Dienstleister lediglich von dort aus eingebunden werden. Außerdem ist zu beachten, dass die JI-RL **keine gemeinsame Verantwortlichkeit zwischen Sicherheitsbehörden und Privaten** erlaubt (vgl. Art. 3 Nr. 8 JI-RL). Private „Dritte“ dürfen daher nur als Auftragsverarbeiter personenbezogene

[7] St. Rspr. des EuGH, Urt. v. 9.11.2010, C-92/09 (Schecke), ECLI:EU:C:2010:662, Rn. 77; Urt. v. 7.11.2013, Rs. C-473/12 (IPI), ECLI:EU:C:2013:715, Rn. 39; Urt. v. 16.7.2020, Rs. C-311/18 (Schrems II), ECLI:EU:C:2020:559, Rn. 176; Jarass, Charta der Grundrechte der Europäischen Union, 4. Aufl., 2021, Art. 8 Rn. 17; Wolff in Pechstein/Nowak/Häde (Hrsg.), Frankfurter Kommentar EUV/GRC/AEUV, 2017, Art. 8 GRCh Rn. 48.

Daten im Zusammenhang mit § 42d ASOG-E verarbeiten.[8] Dies ist gesetzlich klarzustellen. Zudem fehlt eine klare Begrenzung auf nicht-sensible personenbezogene Daten.

Weiterhin besteht die Gefahr, dass trotz (optionaler) Löschung der Trainingsdaten **Rückschlüsse auf die betroffenen Personen** möglich bleiben. In die Vorschrift sollte daher ein ausdrückliches Verbot der De-Anonymisierung aufgenommen werden – eine Forderung, die auch die Datenethikkommission der Bundesregierung in anderem Zusammenhang bereits erhoben hat.[9]

Schließlich bedarf es einer Klarstellung, wie § 42d ASOG-E im **Verhältnis zu den allgemeinen datenschutzrechtlichen Vorgaben** steht. Um das durch die JI-RL und das BlnDSG garantierte hohe Schutzniveau nicht zu unterlaufen, sollte in der Norm ausdrücklich festgehalten werden, dass sie keine abschließende Regelung darstellt. Insbesondere müssen die allgemeinen Informationspflichten und Betroffenenrechte unberührt bleiben.

D. Automatisierte Anwendung zur Analyse vorhandener Daten (§ 47a ASOG-E)

Der Gesetzentwurf führt mit § 47a ASOG-E eine neue Befugnisnorm für automatisierte Datenanalysen (**Data-Mining**) bei der Berliner Polizei ein. Solche modernen Analysemethoden können zweifellos einen wichtigen Beitrag zur Weiterentwicklung der Gefahrenabwehr leisten – insbesondere in einer zunehmend datafizierten Gesellschaft. Ihre Einführung wirft jedoch erhebliche grundrechtliche[10] Fragen auf, die einer sorgfältigen Prüfung bedürfen.[11]

---

[8] Vgl. Martini/Kemper, CR 2023, 414 (417).

[9] Datenethikkommission, Gutachten, S. 132.

[10] Vorrangiger Prüfungsmaßstab sind trotz JI-RL (und KI-VO) die Vorschriften des Grundgesetzes und nicht der GRCh. Vgl. dazu z.B. Hofmann-Coombe, EuR 2025, 363 (363 ff.).

[11] Dazu ausführlich Martini/Botta, Polizeiliche Datenanalyse mittels KI: Unions-, polizei- und verfassungsrechtliche Vorgaben, 2025 (in Vorbereitung).

I. Verfassungskonformität

Die Verfassungskonformität des § 47a ASOG-E bestimmt sich in erster Linie danach, inwieweit die Vorschrift die **bundesverfassungsgerichtlichen Maßstäbe zum polizeilichen Data-Mining** einhält. Konkret hat das BVerfG im Jahr 2023 die Ermächtigungsgrundlagen des § 25a HSOG (Automatisierte Anwendung zur Datenanalyse)[12] und des § 49 HmbPolDVG (Automatisierte Anwendung zur Auswertung vorhandener Daten) geprüft und in Teilen für verfassungswidrig befunden.[13] Der Berliner Gesetzentwurf orientiert sich nunmehr an den reformierten Vorschriften aus Hessen und Hamburg.

1. Grundrechtseingriff

Werden gespeicherte Datenbestände mittels einer automatisierten Anwendung zur Datenanalyse verarbeitet, greift dies in das Grundrecht auf **informationelle Selbstbestimmung** (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) aller ein, deren Daten bei diesem Vorgang personenbezogen Verwendung finden.[14] Mit der automatisierten Auswertung gespeicherter Daten erlaubt § 47a ASOG-E eine weitere Nutzung früher erhobener Daten über den ursprünglichen Anlass hinaus. Das begründet einen neuen Grundrechtseingriff und muss verfassungsrechtlich eigens nach dem **Grundsatz der Zweckbindung** gerechtfertigt werden.[15] Indessen liegt ein Grundrechtseingriff hier nicht nur in der weiteren, zusammenführenden Verwendung vormals getrennter Daten, sondern darüber hinaus in der Erlangung besonders grundrechtsrelevanten **neuen Wissens**, das durch die automatisierte Datenanalyse geschaffen werden kann.[16]

---

[12] Weiterführend z.B. Santhakumar, „Legal Design“ für HessenData (§ 25a HSOG) – ein abgestuftes Kontrollkonzept, in: Botta et al. (Hrsg.), Rechtsfragen virtueller Welten, 2025, S. 103 (105 ff.).

[13] BVerfGE 165, 363 (363 ff.).

[14] BVerfGE 165, 363 (388).

[15] BVerfGE 165, 363 (388); vgl. BVerfGE 141, 220 (324 und 327).

[16] BVerfGE 165, 363 (388 f.); Graulich, NVwZ-Beilage 2023, 27 (30); vgl. BVerfGE 156, 11 (39 f.).

2. Rechtfertigung

Der Grundrechtseingriff durch die automatisierte Datenanalyse lässt sich jedoch grundsätzlich rechtfertigen.[17] Dies hängt insbesondere von der **materiellen Verfassungsmäßigkeit** des § 47a ASOG-E, d.h. von seiner Verhältnismäßigkeit.

a) Legitimer Zweck, Geeignetheit und Erforderlichkeit

§ 47a ASOG-E dient dem legitimen Zweck der polizeilichen Aufgabenerfüllung. Die Vorschrift ist zu diesem Zweck auch förderlich, d.h. geeignet. Mangels gleich geeigneter, milderer Mittel ist § 47a ASOG-E erforderlich. Insbesondere zeichnen sich automatisierte Datenanalysen im **Unterschied zu manuellen Datenabgleichen** dadurch aus, dass sie darauf gerichtet sind, neues Wissen zu erzeugen. Unter Zeitdruck lassen sich die stetig wachsenden Datenmengen zudem überhaupt nur noch schwer manuell auswerten.[18]

b) Angemessenheit

Spezielle Anforderungen für die automatisierte Datenanalyse durch Polizeibehörden ergeben sich aus dem Gebot der Angemessenheit. Wie streng diese Anforderungen im Einzelnen sind, bestimmt sich nach dem **Eingriffsgewicht der Maßnahme**.[19] Das Eingriffsgewicht einer automatisierten Datenanalyse und die Anforderungen an deren verfassungsrechtliche Rechtfertigung hängen zum einen vom **Gewicht der vorausgegangenen Datenerhebungseingriffe** ab.[20] Dann sind die Grundsätze der Zweckbindung und Zweckänderung maßgeblich. Zum anderen hat die automatisierte Datenanalyse ein **Eigengewicht**, da die Weiterverarbeitung spezifische Belastungen mit sich bringen

[17] BVerfGE 165, 363 (388).

[18] Vgl. BVerfGE 165, 363 (389).

[19] stRspr. des BVerfG, siehe BVerfGE 165, 363 (389); Graulich, NVwZ-Beilage 2023, 27 (31); vgl. BVerfGE 141, 220 (269).

[20] BVerfGE 165, 363 (390).

kann, die über das Eingriffsgewicht der ursprünglichen Datenerhebung hinausgehen.[21] In diesem Zusammenhang ergeben sich aus dem Gebot der Angemessenheit zusätzliche Rechtfertigungsanforderungen.

aa) Eingriffsintensität der Datenanalyse

Diese weitergehenden Rechtfertigungsanforderungen an eine automatisierte Datenanalyse variieren nach deren Eingriffsintensität.[22] Der Gesetzgeber kann den Umfang der Rechtfertigungsanforderungen daher bewusst steuern, indem er die maßgeblichen Faktoren für die Eingriffsintensität regelt.

(1) Art und Umfang der verarbeitbaren Daten

Das Eingriffsgewicht wird insbesondere durch **Art und Umfang der verarbeitbaren Daten** bestimmt.[23] Je größer die **Menge an personenbezogenen Daten** ist, die in die automatisierte Datenanalyse einbezogen werden kann – und je weniger der Gesetzgeber die verwendbare Datenmenge begrenzt –, desto schwerer wiegt der Eingriff.[24] Dabei ist die Regelung der Menge der verwendbaren Daten eng mit der Festlegung der Art der Daten verknüpft. Je weniger die Art der verwendbaren Daten eingeschränkt wird, desto größer fällt die verarbeitbare Datenmenge aus, was tendenziell das Eingriffsgewicht erhöht.[25]

(a) Herkunft der Daten

Das Eingriffsgewicht kann durch gesetzliche Regelungen zur Herkunft der Daten verringert werden: bspw. durch eine Beschränkung auf Daten, die von der Behörde selbst oder von einer anderen

[21] BVerfGE 165, 363 (390); Bäuerle, ZD 2025, 128 (130).

[22] BVerfGE 165, 363 (398).

[23] BVerfGE 165, 363 (401 ff.).

[24] BVerfGE 165, 363 (401).

[25] BVerfGE 165, 363 (401).

Behörde desselben Landes – zumindest jedoch einer anderen **inländischen Behörde** – erhoben wurden.[26] Auch der Ausschluss von Daten aus **sozialen Netzwerken** oder der Ausschluss von Daten, die von **nachrichtendienstlichen Behörden** stammen, kann die Eingriffsintensität abmildern.[27]

Gemessen an diesen Vorgaben bewirkt § 47a Abs. 2 S. 1 ASOG-E zwar eine gewisse Reduzierung des Eingriffsgewichts, aber nicht in einem Ausmaß, das die gebotenen Rechtfertigungsanforderungen absenken würde. Konkret können Vorgangsdaten, Falldaten, Daten aus den polizeilichen Auskunftssystemen, Nutzungsdaten, Telekommunikationsdaten, Daten aus Asservaten, Daten aus dem polizeilichen Informationsaustausch, soweit sie der polizeilichen Aufgabenerfüllung dienen und in den Fällen des § 47a Abs. 1 S. 2 Nr. 1 ASOG-E auch Verkehrsdaten weiterverarbeitet werden. Außerdem ist es der Polizei erlaubt, personenbezogene Daten aus gezielten Abfragen in gesondert geführten staatlichen Registern (z.B. Melde- oder Waffenregister) in der Analyseplattform zusammenzuführen (§ 47a Abs. 2 S. 2 ASOG-E). Die begrenzende Wirkung dieser Vorgaben dürfte maßgeblich davon abhängen, inwieweit die betroffenen **personenbezogenen Daten gekennzeichnet** sind. Zwar sieht **§ 42b ASOG-E** eine grundsätzliche Kennzeichnungspflicht vor, diese wird aber durch weitgehende Ausnahmeregelungen erheblich abgeschwächt.[28]

Vor allem die Einbeziehung von **Vorgangsdaten** trägt erheblich zum Volumen der Datenanalyse bei.[29] Ein „Vorgang“ umfasst sämtliche Unterlagen, die im Zusammenhang einer polizeilichen Tätigkeit über eine bestimmte Person, Sache oder einen sonstigen Gegenstand polizeilichen Handelns geführt werden.[30] In den Vorgangsbearbeitungssystemen erfasst die Polizei Daten, die sie für ihre konkrete polizeiliche Aufgabe und Sachbearbeitung im Einzelfall benötigt. Aufgenommen werden insbesondere Anzeigen, Ermittlungsberichte und Vermerke (auch zu Verkehrsunfällen). Die Systeme enthalten auch Daten zu Personen, die Anzeige erstatten oder Hinweise geben, zu Zeugen,

---

[26] BVerfGE 165, 363 (401).

[27] BVerfGE 165, 363 (401).

[28] Vgl. BVerfGE165, 363 (424).

[29] Vgl. BVerfGE 165, 363 (422).

[30] Müller/Schwabenbauer, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 7. Aufl. 2021, Abschnitt G, Rn. 832 m.w.N.

Unfallbeteiligten und anderen Personen, die nicht Verdächtige oder Beschuldigte i.S.d. Strafprozessrechts oder Verantwortliche i.S.d. Polizeirechts sind. Hervorzuheben ist daher, dass die Vorgangsdaten von **Unbeteiligten**[31] nicht in die Datenanalyse einfließen sollen (§ 47a Abs. 2 S. 5 ASOG-E).

Eingriffsmildernd wirkt darüber hinaus, dass eine direkte Anbindung der Analyseplattform **an Internetdienste** unzulässig ist (§ 47a Abs. 2 S. 3 ASOG-E). Eine Relativierung erfährt dieses Verbot indes durch § 47a Abs. 2 S. 4 ASOG-E, wonach die Polizei einzelne gesondert gespeicherte Datensätze aus Internetquellen (z.B. Social Media oder Online-Foren) ergänzend auf der Analyseplattform zusammenführen kann.[32]

Eine herkunftsbezogene Beschränkung auf Daten, die ursprünglich **durch inländische Polizeibehörden** erhoben worden sind, findet sich in der Regelung **nicht** niedergelegt. So dürfte es bspw. zulässig sein, personenbezogene Daten, die **Nachrichtendienste** an Polizeibehörden übermittelt haben (z.B. nach § 19 BVerfSchG, § 11 BNDG oder § 11 MADG) und sich somit nunmehr in den polizeilichen Datenbeständen befinden, in eine Analyseplattform nach § 47a ASOG-E einzuspeisen.

Auch ist die Verarbeitung von Daten, die ursprünglich **durch besonders schwere Grundrechtseingriffe** erlangt wurden, z.B. durch die Wohnraumüberwachung oder den Einsatz Verdeckter Ermittler nicht generell ausgeschlossen (vgl. § 47a Abs. 2 S. 6 ASOG-E).

Da § 47a Abs. 2 S. 1 ASOG-E ausdrücklich die Verarbeitung von Telekommunikationsdaten einschließt, ist neben der informationellen Selbstbestimmung auch das **Fernmeldegeheimnis des Art. 10 Abs. 1 Var. 3 GG** („Telekommunikationsgeheimnis“) berührt.

---

[31] Personen, zu denen keine tatsächlichen Anhaltspunkte vorliegen, dass sie selbst in Straftaten verwickelt sind bzw. Kontakt zu einer solchen Person haben; hierzu gehören Tatopfer sowie Zeuginnen und Zeugen. Siehe AGH-Drs. 19/2553, S. 333.

[32] Vgl. Zöller, Schriftliche Stellungnahme zum Gesetzentwurf der Landesregierung für ein Landesgesetz zur Änderung des Polizei- und Ordnungsbehördengesetzes vom 6. November 2024 (RLP-LT-Drs. 18/10756), S. 18.

(b) Datenarten und -formate

Eine Chance zur Eingriffsmilderung verpasst der Gesetzentwurf, indem er keine Regelung zu den **zugelassenen Datenarten** (vgl. etwa § 3 Abs. 1 ATDG oder § 29 Abs. 2a S. 3 GwG) beinhaltet.[33] Auch eine Regelung der **einbeziehbaren Dateiformate** (Bilder, Video- und Audioaufnahmen) oder ein **Ausschluss biometrischer Daten** finden sich in § 47a ASOG-E nicht. Eine damit einhergehende Eingriffsmilderung kann erst aus den Verwaltungsvorschriften nach § 47a Abs. 6 ASOG-E erfolgen. Getreu der **Wesentlichkeitstheorie** sollte es der parlamentarische Gesetzgeber sein, der klare Leitplanken für die Datenauswahl aufstellt. Aus Rechtsschutzperspektive wäre jedenfalls die Rechtsform der **Rechtsverordnung** gegenüber der Verwaltungsvorschrift vorzugswürdig.[34]

(c) Entstehung einer „Super-Datenbank“

Als das BVerfG über die Verfassungsmäßigkeit der Ermächtigungsgrundlagen aus Hamburg und Hessen entschieden hat, hatte es erkennbar keine **dauerhafte Zusammenführung der polizeilichen Datenbestände**, sondern vielmehr eine anlassbezogene Zusammenführung zwecks automatisierter Datenanalyse vor Augen.[35] § 47a Abs. 1 S. 1 ASOG-E soll jedoch eine dauerhafte Zusammenführung, Verknüpfung und Aufbereitung personenbezogener Daten auf einer Analyseplattform erlauben; m.a.W.: die **Entstehung einer „Super-Datenbank“**. Der damit einhergehende Grundrechtseingriff ist nicht nur von eigenem Gewicht,[36] sondern derart gewichtig, dass die Norm schon aus diesem Grund **verfassungswidrig** ist.[37] Denn im Unterschied zur konkreten Datenanalyse stellt § 47a ASOG-E für die vorsorgende Datenzusammenführung, -verknüpfung und

---

[33] Vgl. BVerfGE 165, 363 (404).

[34] Vgl. BVerfGE 165, 363 (414).

[35] Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Stellungnahme zum Entwurf eines Gesetzes zur Verbesserung der Terrorismusbekämpfung, BT-Drs. 20/12806, Ausschuss-Drs. 20(4)483, S. 8.

[36] Vgl. Bäuerle, in: BeckOK PolR Hessen, 33. Ed. 1.6.2024, HSOG § 25a Rn. 100; zum Eingriffsgewicht einer heimlichen, vorsorgenden Datenspeicherung siehe BVerfG, NVwZ 2024, 1736 (1748 ff.).

[37] Vgl. Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Stellungnahme zum Entwurf eines Gesetzes zur Verbesserung der Terrorismusbekämpfung, BT-Drs. 20/12806, Ausschuss-Drs. 20(4)483, S. 8; Kipker, Schriftliche Stellungnahme zum Entwurf eines Gesetzes zur Verbesserung der Terrorismusbekämpfung, BT-Drs. 20/12806, Ausschuss-Drs. 20(4)493 J, S. 15 f.

-aufbereitung jenseits der anlassbezogenen Analyse **keine eigenen Rechtmäßigkeitsvoraussetzungen** auf – erst recht keine, die den Maßstäben des BVerfG für heimliche Überwachungsmaßnahmen genügen würden (insbesondere das Erfordernis einer zumindest hinreichend konkretisierten Gefahr für besonders gewichtige Rechtsgüter).

(2) Zugelassene Methode der Datenanalyse

Zusätzlich beeinflusst die zugelassene Methode der Datenanalyse die Eingriffsintensität.

(a) Komplexität des Datenabgleichs

Besonders hohe Eingriffsintensität kann der Einsatz komplexer Methoden des Datenabgleichs haben.[38] Wenn die Polizei mithilfe aller verfügbaren informationstechnischen Möglichkeiten aus den vorhandenen Daten weitreichende Erkenntnisse gewinnt, neue Zusammenhänge erschließt, durch mehrstufige Analysen neue Verdachtsmomente erzeugt und daraufhin weitere Analyseschritte oder operative Maßnahmen einleitet, können die negativen Auswirkungen einer automatisierten Datenanalyse für die Betroffenen erheblich sein.[39] Das Gewicht der individuellen Beeinträchtigung wird dadurch deutlich erhöht. Bei komplexen Datenabgleichen kommt hinzu, dass die Möglichkeit, Fehler zu erkennen und zu korrigieren, erschwert wird – vor allem aufgrund der **mangelnden Nachvollziehbarkeit der eingesetzten Algorithmen**.[40] Dies erschwert Rechtsschutz und externe Kontrolle erheblich. Eine zusätzliche Herausforderung besteht darin, die Entstehung und Nutzung **diskriminierender Algorithmen** zu verhindern. Wird Software von **privaten Akteuren oder ausländischen Staaten** eingesetzt, steigt zudem das Risiko unbemerkter Manipulation oder des unerkannten Zugriffs auf Daten durch Dritte.[41] Insgesamt ist die Methode der automatisierten Datenanalyse umso eingriffsintensiver, je mehr und tiefere Erkenntnisse über Personen erlangt

[38] BVerfGE 165, 363 (404).

[39] BVerfGE 165, 363 (404 f.).

[40] BVerfGE 165, 363 (405); vgl. BVerfGE 154, 152 (259 f.).

[41] BVerfGE 165, 363 (408).

werden können, je höher die Anfälligkeit für Fehler und Diskriminierung ist und je schwerer die softwaregestützten Verknüpfungen nachvollzogen werden können.[42]

Vor diesem Hintergrund ist es entscheidend, dass § 47a ASOG-E den **Einsatz von KI-Systemen** erlaubt und damit auch komplexe Verarbeitungsmethoden zulässt. Dem steht nicht entgegen, dass die Datenanalyse manuell ausgelöst werden und regelbasiert auf einer von Menschen definierten Abfolge von Analyse- und Verarbeitungsschritten ablaufen muss (§ 47a Abs. 1 S. 4 ASOG-E). Daraus folgt allein ein Verbot sogenannter lernender Systeme. Auf diese beschränkt sich die maßgebliche KI-Definition des Art. 3 Nr. 1 KI-VO jedoch nicht. Auch nicht lernfähige Systeme gelten als KI.[43]

(b) Offenheit des Suchvorgangs

Das Eingriffsgewicht ist außerdem umso größer, je offener die Methode des Suchvorgangs ist und je weniger die automatisierte Datenanalyse durch **polizeiliche Suchmuster** gesteuert wird, die auf spezifischen Erkenntnissen und Annahmen zum konkreten Sachverhalt beruhen.[44] Das Eingriffsgewicht steigt insbesondere, wenn die Datenanalyse nicht auf einem **Suchbegriff** basiert, der sich auf den bislang erkennbaren Sachverhalt bezieht – wie es bspw. in § 65a Abs. 2 S. 2 POG RLP vorgesehen ist: „Die automatisierte Datenanalyse wird manuell ausgelöst und erfolgt anhand von Suchbegriffen, die sich aus einem konkreten Sachverhalt, bezogen auf einen Anlass im Sinne des Absatzes 1 ergeben; bei Maßnahmen nach Absatz 1 Nr. 2 und 3 ist der Suchvorgang zudem auf die nach den §§ 4 und 5 Verantwortlichen auszurichten.“ Wenn die Analyse jedoch darauf abzielt, lediglich statistische Auffälligkeiten in den Datenmengen zu entdecken, die anschließend in weiteren automatisierten Abgleichschritten mit bestimmten Datenbeständen verknüpft werden, können daraus neue Informationen entstehen, nach denen die Polizei zuvor keinen Anlass zur Suche hatte.[45] Vor diesem Hintergrund bewirkt § 47a Abs. 1 S. 5 ASOG-E eine Eingriffsmilderung, indem er festhält,

---

[42] BVerfGE 165, 363 (405).

[43] Wendehorst, in: Martini/Wendehorst (Hrsg.), KI-VO, 2024, Art. 3 Rn. 32 ff.; vgl. Benamor, BayVBl 2025, 44 (48 f.).

[44] BVerfGE 165, 363 (405 f.).

[45] BVerfGE 165, 363 (406).

dass nur mit den Suchparametern übereinstimmende Daten angezeigt werden dürfen. Zusätzlich sollte klargestellt werden, dass **diese Parameter anlassbezogen und zielgerichtet** sein müssen.

(c) Art der Suchergebnisse

Das Eingriffsgewicht hängt darüber hinaus davon ab, welche Art von Suchergebnissen durch eine automatisierte Datenanalyse erzielt wird.[46] Besonders eingriffsintensiv erweist es sich, wenn die automatisierte Anwendung **personenbezogene Erkenntnisse** liefert und dabei maschinelle Sachverhaltsbewertungen enthält, die über die bloße Anzeige von Übereinstimmungen zwischen dem Suchkriterium und den durchsuchten Daten hinausgehen.[47] Das gilt vor allem, wenn i.R.v. **Predictive Policing** maschinell Gefährlichkeitsaussagen über Personen getroffen werden. Diesbezüglich hält § 47a Abs. 1 S. 6 ASOG-E zwar fest, dass automatisierte Entscheidungsfindungen und Sachverhaltsbewertungen unzulässig sind. Aber auch die menschliche Entscheidung/Bewertung lediglich vorbereitende Aussagen informationstechnischer Systeme können einen grundsensiblen Ankereffekt bewirken.

(3) Zwischenfazit

Im Ergebnis ergeben sich aus § 47a ASOG-E – trotz der begrüßenswerten Anstrengungen, die Eingriffsintensität abzumildern – schwerwiegende Eingriffe in die informationelle Selbstbestimmung. Eine besondere Eingriffsintensität geht von der Schaffung einer „Super-Datenbank“ aus, die schon für sich die Verfassungswidrigkeit der Regelung zur Folge hat.

bb) Rechtfertigungsanforderungen

Ermöglicht die automatisierte Datenanalyse einen **schwerwiegenden Eingriff** in die informationelle Selbstbestimmung, ist dies nach der Rechtsprechung des BVerfG grundsätzlich nur unter den engen Voraussetzungen zu rechtfertigen, wie sie allgemein für eingriffsintensive heimliche

[46] BVerfGE 165, 363 (407).

[47] BVerfGE 165, 363 (407).

Überwachungsmaßnahmen gelten, also nur zum **Schutz besonders gewichtiger Rechtsgüter**, sofern für diese eine **zumindest hinreichend konkretisierte Gefahr** besteht.[48]

(1) Datenanalyse gemäß § 47a Abs. 1 S. 2 Nr. 1 ASOG-E

Der Tatbestand des § 47a Abs. 1 S. 2 Nr. 1 ASOG-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 sexuelle Selbstbestimmung einer Person oder für Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist. Die Ermächtigungsgrundlage ist somit **verfassungskonform**.[49]

(2) Datenanalyse gemäß § 47a Abs. 1 S. 2 Nr. 2 ASOG-E

Anders ist der Tatbestand des § 47a Abs. 1 S. 2 Nr. 2 ASOG-E zu bewerten. Zwar greift die Vorschrift ersichtlich die Rechtsprechung des BVerfG zur zumindest **hinreichend konkretisierten Gefahr** auf, indem tatsächliche Anhaltspunkte die Annahme rechtfertigen müssen, dass innerhalb eines übersehbaren Zeitraumes auf eine zumindest ihrer Art nach konkretisierte Weise eine in § 100a Abs. 2 StPO bezeichnete und voraussichtlich auch im Einzelfall schwerwiegende Straftat begangen werden soll und die Maßnahme zur Verhütung dieser Straftat erforderlich ist. Aber der Regelungsvorschlag verankert damit **lediglich eine Bedingung** der konkretisierten Gefahr im Normtext. Denn zusätzlich müssen die Tatsachen den Schluss darauf zulassen, dass **bestimmte Personen** beteiligt sein werden, über deren Identität zumindest so viel bekannt ist, dass die staatliche Maßnahme gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden kann.[50] Außerdem dient die Regelung nicht allein dem Schutz besonders gewichtiger Rechtsgüter. Straftaten nach § 100a Abs. 2 StPO umfassen u.a. auch **gewerbs- oder bandenmäßig begangene Vergehen**, die sich in erster Linie gegen das

---

[48] BVerfGE 165, 363 (410). Das Erfordernis einer zumindest hinreichend konkretisierten Gefahr für besonders gewichtige Rechtsgüter ist nur dann verfassungsrechtlich verzichtbar, 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 in der Sache so eng begrenzt sind, dass das Eingriffsgewicht der Maßnahmen erheblich gemindert ist.

[49] Vgl. Bäuerle, in: BeckOK PolR Hessen, 33. Ed. 1.6.2024, HSOG § 25a Rn. 32.

[50] BVerfGE 141, 220 (272); 165, 363 (411); BVerfG, NVwZ 2024, 1736 (1742).

Vermögen der Geschädigten richten (z.B. Wohnungseinbruchsdiebstahl nach § 244 StGB; Erpressung nach § 253 StGB etc.). Damit öffnet die Ermächtigungsgrundlage den Rechtsgüterschutz „nach unten“.[51] Dem wirkt auch das ergänzende Erfordernis „und voraussichtlich auch im Einzelfall schwerwiegende Straftat begangen werden soll“ nicht ausreichend entgegen. Denn alle Straftaten i.S.d. § 100a Abs. 2 StPO sind „schwere Straftaten“. Die Vorschrift ist folglich **verfassungswidrig**.[52] Der Gesetzgeber sollte ihren Anwendungsbereich dringend konkretisieren und einen abschließenden Katalog von Straftatbeständen aufnehmen.

(3) Datenanalyse gemäß § 47a Abs. 1 S. 2 Nr. 3 ASOG-E

Die Ermächtigungsgrundlage des § 47a Abs. 1 S. 2 Nr. 3 ASOG-E entspricht den verfassungsrechtlichen Vorgaben. Nach der BKAG-Entscheidung des BVerfG können in Bezug auf **terroristische Straftaten**, die oft durch lang geplante Taten von bisher nicht straffällig gewordenen Einzelnen an nicht vorhersehbaren Orten und in ganz verschiedener Weise verübt werden, Überwachungsmaßnahmen auch dann erlaubt werden, wenn zwar noch nicht ein seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennbar ist, jedoch das **individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie solche Straftaten in überschaubarer Zukunft begehen wird**.[53] Denkbar ist das etwa, wenn eine Person aus einem Ausbildungslager für Terroristen im Ausland nach Deutschland einreist.

(4) Unzureichendes Kontrollkonzept

Der Verhältnismäßigkeitsgrundsatz stellt auch Anforderungen an Transparenz, individuellen Rechtsschutz und aufsichtliche Kontrolle.[54] Entscheidend ist dabei eine **sachgerechte Ausgestaltung der Kontrolle**. Um der möglicherweise hohen Zahl von Maßnahmen Herr zu werden, sind sowohl ein abgestuftes Kontrollkonzept zwischen unabhängigen und behördlichen Datenschutzbeauftragten

---

[51] Vgl. Bäuerle, in: BeckOK PolR Hessen, 33. Ed. 1.6.2024, HSOG § 25a Rn. 35.

[52] Vgl. Ruschemeier, Predictive Policing, in: Ebers (Hrsg.), StichwortKommentar Legal Tech, 2024, Rn. 10b.

[53] BVerfGE 141, 220 (272 f.).

[54] stRspr. des BVerfG, siehe BVerfGE 141, 220 (282) m.w.N.

als auch ein stichprobenartiges Vorgehen zulässig.[55] Die aufsichtlichen Kontrollen sind dabei **regelmäßig durchzuführen** (mindestens alle zwei Jahre), damit sie ihrer Kompensationsfunktion für den schwach ausgestalteten Individualrechtsschutz gerecht werden können (vgl. z.B. § 69 Abs. 1 BKAG).[56] Gemessen an diesen Anforderungen begründet § 47a ASOG-E noch kein ausreichendes Kontrollkonzept.

Zwar ist vorgesehen, dass der behördliche Datenschutzbeauftragte stichprobenartige Kontrollen hinsichtlich der Zugriffsrechte durchführt (§ 47a Abs. 3 S. 5 ASOG-E). Deren Häufigkeit ist aber gesetzlich nicht fixiert. Auch besteht kein verpflichtendes Kontrollregime durch die Berliner Beauftragte für Datenschutz und Informationsfreiheit. Diese ist lediglich vor der Einrichtung oder wesentlichen Änderungen einer Analyseplattform anzuhören (§ 47a Abs. 5 S. 2 ASOG-E). **Spezielle Kontrollpflichten während des Plattformbetriebs** folgen auch nicht aus anderen Vorgaben des allgemeinen Datenschutzrechts, das nur Kontrollrechte der Beauftragten begründet. Ohne Kontrollpflichten kann der Gesetzgeber aber keine Regelmäßigkeit der aufsichtlichen Kontrollen sicherstellen.

3. Fazit

Die aus § 47a ASOG-E folgenden Grundrechtseingriffe sind unangemessen und damit unverhältnismäßig. Die **Norm verstößt im gegenwärtigen Entwurfsstadium gegen das Recht auf informationelle Selbstbestimmung** (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG), da insbesondere die Ermächtigungsgrundlage des § 47a Abs. 1 S. 2 Nr. 2 ASOG-E keine angemessene Eingriffsschwelle vorsieht, die dem Gewicht des mit diesen Maßnahmen verbundenen Eingriffs gerecht wird und weil die gesamte Norm über kein ausreichendes Kontrollkonzept verfügt. Diese Defizite können (und sollten) im weiteren Gesetzgebungsverfahren jedoch noch behoben werden.

[55] BVerfGE 165, 363 (412).

[56] BVerfGE 141, 220 (285).

II. Unionskonformität

Die automatisierte Datenanalyse ruft zusätzlich zum nationalen Verfassungsrecht auch das Unionsrecht auf den Plan. Neben den Vorgaben der JI-RL ist vornehmlich die **Verordnung über künstliche Intelligenz (KI-VO)** zu beachten. Sie ist 2024 in Kraft getreten und gilt auch für öffentliche Stellen der Mitgliedstaaten wie die Polizei unmittelbar.

Die KI-VO **verbietet** den Einsatz bestimmter KI-Systeme generell. Im Kontext von § 47a ASOG-E ist dabei von Relevanz, dass zu den verbotenen KI-Praktiken (zumindest in Teilen) auch **personenbezogenes Predictive Policing** zählt. Konkret untersagt ist das Inverkehrbringen, die Inbetriebnahme für diesen spezifischen Zweck oder die Verwendung eines KI-Systems zur Durchführung von Risikobewertungen in Bezug auf natürliche Personen, um das Risiko, dass eine natürliche Person eine Straftat begeht, ausschließlich auf der Grundlage des Profiling einer natürlichen Person oder der Bewertung ihrer persönlichen Merkmale und Eigenschaften zu bewerten oder vorherzusagen (Art. 5 Abs. 1 lit. d Hs. 1 KI-VO). Die Polizei darf folglich auf Grundlage von § 47a ASOG-E keine Software verwenden, die entsprechend zum Einsatz kommt. Das Verbot gilt indes nicht für KI-Systeme, die dazu verwendet werden, die durch Menschen durchgeführte Bewertung der Beteiligung einer Person an einer kriminellen Aktivität, die sich bereits auf objektive und überprüfbare Tatsachen stützt, die in unmittelbarem Zusammenhang mit einer kriminellen Aktivität stehen, zu unterstützen (Art. 5 Abs. 1 lit. d Hs. 2 KI-VO).

Sind polizeiliche KI-Systeme nicht durch Art. 5 KI-VO verboten, stellt es sie jedoch nicht per se von den Vorgaben der Verordnung frei. Diese richten sich nämlich vornehmlich an sogenannte **Hochrisiko-KI-Systeme** (d.h. an deren Anbieter oder Betreiber i.S.d. Art. 3 KI-VO). Ob ein KI-System als Hochrisiko-KI-System zu bewerten ist, bestimmt sich insbesondere nach Annex III KI-VO. Daraus ergibt sich, dass der polizeiliche KI-Einsatz nicht pauschal als hochriskant gilt. Vielmehr muss ein polizeilich verwendetes KI-System den abschließend genannten Kategorien von Hochrisiko-KI-Systemen unterfallen. Im Kontext von § 47a ASOG-E dürfte vor allem eine Kategorie von Hochrisiko-KI-Systemen relevant sein. Dies sind KI-Systeme, die zur Wahrscheinlichkeitsbewertung der Begehung von Straftaten (soweit diese Risikobewertung nicht nur auf der Grundlage von Persönlichkeitsprofilen gemäß Art. 3 Abs. 4 JI-RL erfolgt) oder zur Bewertung persönlicher Merkmale und Eigenschaften oder vergangenen kriminellen Verhaltens von natürlichen

Personen oder Gruppen verwendet werden sollen (Annex III Nr. 6 lit. d KI-VO). Ist eine polizeilich verwendete Software als Hochrisiko-KI-System einzustufen, sind die umfassenden (produktsicherheitsrechtlichen) Pflichten der Art. 6 ff. KI-VO zu beachten.[57] Unter anderem müssen die Polizeibehörden die entwickelten oder verwendeten KI-Systeme in der EU-Datenbank gemäß Art. 71 KI-VO registrieren.

III. Technische Umsetzung

Auch wenn § 47a ASOG-E technikneutral ausgestaltet ist, lässt sich die Norm nicht gänzlich losgelöst von ihrer technischen Umsetzung bewerten. Aus Gründen der **digitalen Souveränität** ist die **herstellerunabhängige Entwicklung** einer Analyseplattform zu empfehlen. Zu begrüßen ist es, dass das Land Berlin derzeit nicht plant, Anwendungen **des US-amerikanischen Unternehmens Palantir Technologies GmbH** wie „Gotham" einzusetzen.[58] Palantir war in der Vergangenheit wiederholt Gegenstand öffentlicher Kritik. So verweigerte das Unternehmen dem New York Police Department nach Ablauf eines Vertrags den Zugang zu bisherigen Analyseergebnissen, um deren Nutzung mit einer alternativen Softwarelösung von IBM zu verhindern.[59] Zudem gilt der Palantir-Mitgründer Peter Thiel als einflussreicher Vordenker der US-amerikanischen Rechten und fällt regelmäßig durch demokratiekritische Positionierungen auf.[60] Aber auch soweit ein anderes privates IT-Produkt – zumal ein (Hochrisiko-)KI-System – zum Einsatz kommen soll, ist im Normtext zwingend ein ausreichendes **staatliches Monitoring** dieser Software abzusichern.[61] Daran fehlt es bislang.

---

[57] Bäuerle, ZD 2025, 128 (131).

[58] Schriftliche Anfrage, AGH-Drs. 19/23039, S. 1.

[59] Alden, There's A Fight Brewing Between The NYPD And Silicon Valley's Palantir, BuzzFeed News vom 28.6.2017, https://www.buzzfeednews.com/article/williamalden/theres-a-fight-brewing-between-the-nypd-and-silicon-valley#.cfryqemg5.

[60] Göpfert, Trump und Thiels Palantir - gefährliche Allianz? Tagesschau.de vom 9.5.2025, https://www.tagesschau.de/wirtschaft/unternehmen/palantir-trump-thiel-ki-aktie-daten-100.html.

[61] Vgl. BVerfGE 165, 363 (412 f.); Ruschemeier, Predictive Policing, in: Ebers (Hrsg.), StichwortKommentar Legal Tech, 2024, Rn. 10d; Santhakumar, „Legal Design" für HessenData (§ 25a HSOG) – ein abgestuftes Kontrollkonzept, in: Botta et al. (Hrsg.), Rechtsfragen virtueller Welten, 2025, S. 103 (114 f.).