weizenbaum
POLICY PAPER

März 2026
# 19

Weizenbaum-Institut

# Stellungnahme zur Novellierung des Allgemeinen Sicherheits- und Ordnungsgesetzes Berlin (ASOG Bln)

Drucksache 19/2553 und der Änderungsantrag der Fraktion der CDU und der Fraktion der SPD zur Drucksache 19/2553

**AUTOR:INNEN**

**Dr. Jonas Botta** \\ FernUniversität in Hagen \\ Deutsches Forschungsinstitut für öffentliche Verwaltung
**Dr. Dietmar Kammerer** \\ Weizenbaum-Institut e.V.
**Charlotte Mysegades** \\ Weizenbaum-Institut e.V.
**Philipp Schöbel** \\ Humboldt-Universität zu Berlin
**Prof. Dr. Herbert Zech** \\ Humboldt-Universität zu Berlin \\ Weizenbaum-Institut e.V.

Nennung der Autor:innen in alphabetischer Reihenfolge.

Unter Mitarbeit von
**Schabnam Fayeq, Jeremias Gestrich, Helena Zabel** \\ Weizenbaum-Institut e.V.

**Kontakt:** charlotte.mysegades@weizenbaum-institut.de

**ÜBER DIESES PAPER**

Die Stellungnahme wurde in einem kollaborativen Prozess am Weizenbaum-Institut erarbeitet. Im Anschluss an eine Analyse der Vorschriften des Referentenentwurfs folgte die Erarbeitung von Schwerpunkten einer Stellungnahme in arbeitsteiligem Vorgehen der Autor:innen. Anschließend wurde die Stellungnahme von dem Direktorium des Weizenbaum-Instituts im Rahmen der Direktoriumssitzung am 16. März 2026 beschlossen und zur Veröffentlichung freigegeben.

In den Weizenbaum Policy Papers werden wissenschaftlich fundierte Stellungnahmen, Positionspapiere und Briefings zu aktuellen politischen Themen und Entscheidungsprozessen veröffentlicht.

**ÜBER DAS WEIZENBAUM-INSTITUT**

Das Weizenbaum-Institut ist ein Verbundprojekt und wird vom Bundesministerium für Forschung, Technologienfolgenabschätzung und Raumfahrt (BMFTR) und dem Land Berlin gefördert. Es betreibt interdisziplinäre Grundlagenforschung zur digitalen Transformation der Gesellschaft und liefert evidenzbasierte und wertorientierte Handlungsoptionen, damit die Digitalisierung nachhaltig, selbstbestimmt und verantwortungsvoll gestaltet werden kann.

Weizenbaum Policy Paper

# Stellungnahme zur Novellierung des Allgemeinen Sicherheits- und Ordnungsgesetzes Berlin (ASOG Bln)

Drucksache 19/2553 sowie der Änderungsantrag der Fraktion der CDU und der Fraktion der SPD zur Drucksache 19/2553

Weizenbaum-Institut

## Abstract

Mit der im Dezember 2025 beschlossenen Novellierung des Allgemeines Sicherheits- und Ordnungsgesetz Berlin (ASOG Bln) hat das Land Berlin das Polizeirecht umfassend angepasst und neue sowie erweiterte Befugnisse insbesondere im Bereich digitaler Technologien eingeführt. Die Novelle betrifft unter anderem Videoüberwachung, den Einsatz körpernah getragener Kameras, automatisierte Datenanalysen, KI-gestützte Verhaltensauswertungen sowie biometrische Abgleiche mit öffentlich zugänglichen Daten. Diese Maßnahmen berühren in erheblichem Umfang grundrechtlich geschützte Positionen und unterliegen zugleich unionsrechtlichen Vorgaben.

Vor diesem Hintergrund analysiert die Stellungnahme des Weizenbaum-Instituts ausgewählte Regelungen der ASOG-Novelle aus verfassungsrechtlicher, unionsrechtlicher und sozialwissenschaftlicher Perspektive. Sie untersucht insbesondere Eingriffsschwellen, Zweckbindung, Transparenz- und Kontrollmechanismen sowie die rechtlichen und praktischen Folgen des Einsatzes automatisierter Systeme in der Gefahrenabwehr.

Ziel der Stellungnahme ist es, eine evidenzbasierte Einordnung der vorgesehenen Regelungen zu ermöglichen und mögliche Spannungsfelder mit Grundrechten und europäischem Recht aufzuzeigen.

# Inhalt

# 1 Einleitung

Mit der im Dezember 2025 beschlossenen Novellierung des Allgemeinen Sicherheits- und Ordnungsgesetzes (ASOG) wurde das Berliner Polizeirecht in wesentlichen Teilen überarbeitet. Das Weizenbaum-Institut möchte vor dem Hintergrund seiner interdisziplinären Digitalisierungsforschung mit der Stellungnahme zu dem öffentlichen Diskurs beitragen und einzelne der Änderungen analysieren.

Die Stellungnahme wurde in einem kollaborativen Prozess am Weizenbaum-Institut erarbeitet. Auf eine Analyse ausgewählter Vorschriften des Referentenentwurfs folgte die arbeitsteilige Erarbeitung von Schwerpunkten der Stellungnahme durch die Autor:innen. Entsprechend dem interdisziplinären Selbstverständnis des Instituts verbindet sie unterschiedliche Perspektiven.

Ziel dieser Stellungnahme ist es, die Novelle des ASOG aus verfassungsrechtlicher und unionsrechtlicher Perspektive zu beleuchten, unter Einbeziehung sozialwissenschaftlicher und sozio-technischer Erkenntnisse.

## 1.1 Allgemeine Anmerkungen

Die Novelle sieht neue und erweiterte Eingriffsbefugnisse vornehmlich der Polizei Berlin vor, die in erheblichem Umfang grundrechtlich geschützte Sphären berühren. Dies betrifft namentlich das allgemeine Persönlichkeitsrecht, insbesondere in seiner Ausprägung als Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG), den allgemeinen Gleichheitssatz (Art. 3 Abs. 1 GG), die Meinungsfreiheit (Art. 5 Abs. 1 GG), die Versammlungsfreiheit (Art. 8 GG), das Telekommunikationsgeheimnis (Art. 10 Abs. 1 Var. 3 GG) sowie die Unverletzlichkeit der Wohnung (Art. 13 GG). Vor diesem Hintergrund ist es unerlässlich, dass die vorgesehenen Regelungen den verfassungsrechtlich gebotenen Anforderungen an Verhältnismäßigkeit, Normenklarheit, Zweckbindung und Transparenz genügen. An mehreren Stellen sieht das Weizenbaum-Institut Nachbesserungsbedarf.

Der Entwurf führt neue Technologien in die Arbeit der Polizei Berlin ein, darunter Systeme Künstlicher Intelligenz (§§ 24a, 24, 42d) oder Plattformen zur Datenaggregation und -analyse (§ 47a). Für bereits im Einsatz befindliche Technologien werden bestehende Erlaubnistatbestände ausgeweitet, so etwa die Ausweitung der Videoüberwachung gefährdeter Objekte (§ 24a) und die dauerhafte optische Überwachung sowie die automatisierte Verhaltensauswertung der Bildaufnahmen an sogenannten „kriminalitätsbelasteten Orten“ (§ 24e). Die Novelle enthält den umfangreichsten Katalog von Änderungen seit der Bekanntmachung des ASOG im Jahr 1975.

## 1.2 Sozialwissenschaftliche Erwägungen

Das Weizenbaum-Institut möchte mit seiner Stellungnahme den interdisziplinären Diskurs zur Novellierung des ASOG stärken und daran erinnern, dass aus sozialwissenschaftlicher

Perspektive der Einsatz von Technik im Sicherheitsbereich niemals alternativlos ist.[1] Technologische Verheißungen führten bereits zu Novellen im Polizei- und Ordnungsrecht mehrerer Bundesländer. Technologische Machbarkeit heißt jedoch nicht Notwendigkeit ihrer Umsetzung.[2] Während der Einsatz von neuer Technik und Technologie möglicherweise Sicherheits- und Effizienzversprechen leisten kann, produziert ihr Einsatz *realiter* neue Abhängigkeiten, Kosten und Risiken: Abhängigkeiten von Hersteller:innen, die insbesondere bei proprietären digitalen Systemen unausweichlich sind; Risiken durch erhöhte Mensch-Technik-Interaktion in Form von Systemausfällen, menschlichen Bedienungsfehlern oder gezieltem Missbrauch; Kosten in der Anschaffung, aber vor allem in der Wartung von Technik sowie in der Ausbildung des Personals.

Der Einsatz von Künstlicher Intelligenz (KI) verschärft die oben genannten Probleme noch. KI ist eine sich hochdynamisch entwickelnde Technologie. Bei den meisten auf dem Markt befindlichen KI-Systemen gilt, dass ihre inneren Operationen weitgehend unverstanden sind, ihre weiteren Entwicklungen unabsehbar sind, ihr Einsatz in der Praxis unerprobt, ihre Fehleranfälligkeit hoch ist und ihr starke Diskriminierungsrisiken inhärent sind. Das European Crime Prevention Network zählt zu den Risiken des polizeilichen Einsatzes von KI: mangelnde Transparenz („black box“), Diffusion von Verantwortung („accountability“), Diskriminierung („bias“) sowie die Tendenz, dass Menschen maschinelle Entscheidungsvorschläge nicht mehr hinterfragen („automation bias“).[3]

Außerdem ist derzeit noch nicht ausreichend geklärt, ob die KI-gestützte Verhaltenserkennung technisch ausreichend zuverlässig funktioniert, zu mehr Effizienz in der Polizeiarbeit führt und die Zahl der Gewalttaten im beobachteten Raum sogar zu senken vermag.[4] Es gehört zum Schicksal der „early adopters“ einer Technologie, dass sie als „Betatester der Industrie“ operieren.

Vor dem Hintergrund, dass das ASOG den Einsatz von KI-Systemen im Zusammenhang mit Grundrechtseingriffen vorsieht, bringt der Einsatz von KI durch die Sicherheitsbehörden in besonderer Weise den von Golla beschriebenen *„Grundkonflikt zwischen der Dynamik technischer Entwicklungen und der notwendigen Bestimmtheit von Eingriffsbefugnissen“*[5] zum Tragen. Das Weizenbaum-Institut empfiehlt daher im Zusammenhang mit ihrer Anwendung im Gefahrenabwehrrecht die abwartende Beobachtung von technischen und

---

[1] Ammicht Quinn, R., Koch, H. A., & Internationales Zentrum für Ethik in den Wissenschaften (IZEW) (Hrsg.). (2015). Intelligente Videoüberwachung: Eine Handreichung. Universitätsbibliothek Tübingen. https://doi.org/10.15496/publikation-8519.

[2] Vgl. Sabine Müller (24.01.25): Polizei und Feuerwehr sollen trotz kritischer Studie flächendeckend Bodycams bekommen. RBB24. https://www.rbb24.de/politik/beitrag/2025/01/berlin-polizei-feuerwehr-bodycams-kritik-studie-einfuehrung.html

[3] European Crime Prevention Network (EUCPN). (2022). *Artificial Intelligence and predictive policing: Risks and challenges* [Recommendation Paper]. https://eucpn.org/sites/default/files/document/files/PP%20%282%29.pdf.

[4] Beim Hamburger Pilotprojekt IVBeo wurden im Evaluationszeitraum 1.140 Hinweise durch KI generiert. Davon wurden nur 11 als polizeilich relevant eingestuft. Vgl. Senat der Hansestadt Hamburg. (2025). *Einsatz künstlicher Intelligenz bei der Überwachung des Hansaplatz (VII)* (Drucksache No. 22/17455; Kleine Anfrage). Bürgerschaft der Freien und Hansestadt Hamburg, dort S. 4.

[5] Sebastian Golla; Lernfähige Systeme, lernfähiges Sicherheitsrecht, S. 9; 2020.

technologischen Entwicklungen und eine wissenschaftliche Evaluierung unter Einbeziehung der Betroffenenperspektive.

# 2 Datenerhebung an und in gefährdeten Objekten (§ 24a ASOG)

Die vorgesehene Regelung zur Datenerhebung an und in einem gefährdeten Objekt, insbesondere einem Gebäude, auch einem Amts- oder Dienstgebäude, einschließlich der jeweils zugehörigen Parkplätze und sonstigen Außenflächen, ermöglicht den Einsatz technischer (Video-)Überwachung an und in den genannten Objekten, *wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass an oder in einem Objekt dieser Art Straftaten drohen.*

Die Norm knüpft damit nicht an das Vorliegen einer konkreten Gefahr an, sondern stellt allein auf tatsächliche Anhaltspunkte für eine abstrakte Gefährdungslage ab. Die Eingriffsschwelle verbleibt folglich auf einem Niveau, das verfassungsrechtlich problematisch ist. Das Recht auf informationelle Selbstbestimmung umfasst die Befugnis des Einzelnen, in aller Regel selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden, und daher grundsätzlich selbst über die Preisgabe und Verwendung persönlicher Daten zu bestimmen.[6] Das Bundesverfassungsgericht hat wiederholt hervorgehoben, dass bereits die offene Videoüberwachung des öffentlichen Raums einen Eingriff in das Recht auf informationelle Selbstbestimmung darstellt, da sie geeignet ist, das Verhalten der Betroffenen zu beeinflussen und die erhobenen Bilddaten zur Erstellung von Bewegungs- und Verhaltensprofilen herangezogen werden können.[7]

Ein Grundrechtseingriff liegt somit bereits dem Grunde nach vor. Dessen Intensität erhöht sich durch die Novelle jedoch aufgrund der in § 24a ASOG vorgesehenen Ausweitung des Anwendungsbereichs auf Amts- und Dienstgebäude, einschließlich ihrer Innenräume sowie der jeweils zugehörigen Parkplätze und sonstigen Außenflächen. Damit geht eine deutliche Intensivierung der bisherigen Befugnisse zur Überwachung und Speicherung einher. Betroffen sind insbesondere das allgemeine Persönlichkeitsrecht in seinen Ausprägungen als Recht am eigenen Bild sowie als Recht auf informationelle Selbstbestimmung, da Personen gefilmt und Bildaufnahmen gespeichert werden.[8]

Hinsichtlich der Erweiterung der Aufzählung gefährdeter Objekte um Amts- und Dienstgebäude fehlt es aus Sicht des Weizenbaum-Instituts in der Gesetzesbegründung an einer Auseinandersetzung mit der Frage, auf welcher empirischen Grundlage Amts- und

[6] Vgl. BVerfG, Beschluss vom 23.02.2007, Az. 1 BvR 2368/06 und Urteil vom 15.12.1983, Az. 1 BvR 209/83.

[7] Vgl. BVerfG, Beschl. v. 23.02.2007 – 1 BvR 2368/06, Rn. 37 f.

[8] Pewestorf/Söllner/Tölle/PolOrdR, 2022, § 24a, Rn.1.; vgl. VGH Mannheim, Urt. V. 21.07.2003 – 1 S 377/02.

Dienstgebäude generell als *gefährdete Objekte* einzustufen sind. Die erforderliche Evidenz für eine derart weitgehende Typisierung bleibt unbeantwortet.

Die Eingriffsintensität nimmt insbesondere durch die Möglichkeit der automatisierten Auswertung der angefertigten Bildaufnahmen und -aufzeichnungen weiter zu.[9] Zwar wird in der Gesetzesbegründung eine biometrische Fernidentifizierung ausdrücklich ausgeschlossen, gleichwohl bleibt die grundrechtliche Belastung erheblich. In der Gesetzesbegründung heißt es hierzu: *„Absatz 1 Satz 2 verweist auf den künftigen § 24e Absatz 4 ASOG. Dadurch kann die Möglichkeit, zur Unterstützung der Einsatzkräfte aus Bildaufnahmen und -aufzeichnungen automatisiert Verhaltensmuster zu erkennen, auch bei der Datenerhebung an gefährdeten Objekten genutzt werden.“*

Die automatisierte Verhaltensmustererkennung wird somit ausdrücklich als Ziel der Maßnahme benannt.[10] Dies wirft Fragen der Normenklarheit und Bestimmtheit auf und erschwert die Vorhersehbarkeit staatlichen Handelns für die Betroffenen.

Hinzu tritt die Verlängerung der Löschfrist für angefertigte Aufnahmen auf einen Zeitraum von bis zu einem Monat (§ 24a Abs. 3 ASOG-E), *„soweit die Daten nicht zur Verfolgung von Straftaten benötigt werden oder Tatsachen die Annahme rechtfertigen, dass die Person künftig Straftaten von erheblicher Bedeutung begehen wird“.* Damit wird eine nachträgliche Auswertung ermöglicht, die über den unmittelbaren Gefahrenabwehrzweck hinausgeht. Nach bisheriger Rechtslage waren Bildaufnahmen unverzüglich zu löschen.[11] Laut der Gesetzesbegründung handelt es sich um eine spezielle Regelung zur zweckändernden Weiterverarbeitung, die die allgemeine Regelung verdrängt. Die Verlängerung der Speicherdauer erfolgt jedoch ohne erkennbar dargelegten sachlichen Grund und steht in Spannung zum verfassungsrechtlich verankerten Zweckbindungsgrundsatz. Damit tritt neben den präventiven Zweck der Gefahrenabwehr ein repressiver Verwendungszweck hinzu, ohne dass dieser auf bestimmte, besonders gewichtige Rechtsgüter begrenzt wäre. Der Kreis der geschützten Rechtsgüter wird vielmehr entgrenzt, da die Norm auf die Verfolgung von *Straftaten* insgesamt abstellt.

Mit dieser zweckändernden Weiterverarbeitung geht zugleich eine Steigerung der Eingriffsintensität einher. Während Betroffene im Kontext präventiver Videoüberwachung regelmäßig von einer anonymen Erfassung ausgehen können, wird diese Erwartung durch die Möglichkeit einer nachträglichen strafverfolgungsbezogenen Nutzung der Daten erheblich relativiert. Die Formulierung *„die Person“* deutet auf einen individualisierenden Zugriff hin, ohne die hierfür erforderlichen Voraussetzungen normenklar zu bestimmen. Für die Betroffenen wird damit nicht mehr hinreichend vorhersehbar, ob und unter welchen

[9] Vgl. § 24a Abs. 1 S. 2 ASOG; Stellungnahme der Berliner Beauftragten für Datenschutz und Informationsfreiheit zum Gesetzesentwurf zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, S.2.

[10] Vgl. weitere Ausführungen zur automatisierten Verhaltensmustererkennung weiter unten.

[11] Vgl. § 24a Abs. 3 ASOG a.F.

Umständen eine Identifizierung und weitergehende Verwendung der sie betreffenden Daten erfolgt.[12]

Vor diesem Hintergrund erscheint zumindest zweifelhaft, ob die mit der zweckändernden Weiterverarbeitung verbundene Erhöhung der Eingriffsintensität, insbesondere in Verbindung mit der zugleich abgesenkten Eingriffsschwelle und der Ausweitung des geschützten Rechtsgüterkreises, noch den verfassungsrechtlichen Anforderungen des Verhältnismäßigkeitsgrundsatzes genügt.

- Aus Sicht des Weizenbaum-Instituts bedarf die Maßnahme daher engerer tatbestandlicher Voraussetzungen, insbesondere des Vorliegens einer konkreten Gefahr, um eine automatisierte Auswertung der angefertigten Bildaufnahmen und -aufzeichnungen zu rechtfertigen.

- Zudem wäre eine unabhängige und regelmäßige Evaluierung der Wirksamkeit sowie der Auswirkungen auf die Grundrechte ausdrücklich zu begrüßen. Eine solche evidenzbasierte Überprüfung ist Voraussetzung für die Wahrung des Verhältnismäßigkeitsgrundsatzes und kann zugleich das Vertrauen der Bevölkerung in die Entscheidungen des Gesetzgebers stärken.

- Aus Sicht des Weizenbaum-Instituts sollte der Gesetzgeber die Voraussetzungen für eine über die Regellöschfrist hinausgehende Speicherung und Weiterverarbeitung der erhobenen Daten normenklar präzisieren. Insbesondere bedarf es einer eindeutigen Bestimmung, auf welche *Person* sich die in § 24a Abs. 3 ASOG vorgesehene Prognose bezieht und welche Tatsachen einen hinreichend individualisierten Zusammenhang zwischen der betroffenen Person und der künftig zu begehenden Straftat begründen müssen. Eine Speicherung sollte nur in Betracht kommen, wenn sich die Prognose auf eine konkret identifizierbare oder zumindest eindeutig individualisierbare Person bezieht und auf nachvollziehbaren, dokumentierten Tatsachen beruht.

- Darüber hinaus erscheint eine ausdrückliche Begrenzung auf die Verfolgung von Straftaten von erheblicher Bedeutung geboten. Eine pauschale Öffnung für die Verfolgung von *Straftaten* insgesamt führt zu einer Entgrenzung des Verwendungszwecks und erhöht die Eingriffsintensität erheblich. Der Gesetzgeber sollte daher klarstellen, dass eine Weiterverarbeitung zu repressiven Zwecken nur bei Vorliegen besonders gewichtiger Rechtsgüter zulässig ist und den präventiven Charakter der Maßnahme nicht unterläuft.

[12] Sußner, *Try harder hilft selten: Eine verfassungsrechtliche Einordnung der Videoüberwachung an kriminalitätsbelasteten Orten, VerfBlog*, 2026/1/08, https://verfassungsblog.de/berlin-asog-novelle-kbos/, DOI: 10.59704/7bd1f58e3170253a.

# 3 Bild- und Tonaufnahmen und -aufzeichnungen zur Eigensicherung und zum Schutz von Dritten (§ 24c ASOG)

Mit § 24c ASOG wird der Einsatz körpernah getragener Kameras (sogenannter Body-Cams) durch Polizeivollzugs- und Ordnungsbehörden erheblich ausgeweitet. Die Rechtsgrundlage des § 24c ASOG erlaubt es insbesondere den Einsatzkräften der Polizei, der Feuerwehr und des Rettungsdienstes, Body-Cams 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.[13] Das kann in vielen Fällen entscheidend dafür sein, dass der Beauftragte seinen gesetzlichen Auftrag als unabhängige Ombudsperson erfüllen kann.

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 Body-Cam-Aufnahmen nach Einleitung eines Ermittlungsverfahrens ausschließlich diesem Verfahren zugeordnet sind. Das bedeutet: Nicht mehr die Polizei, sondern die Staatsanwaltschaft müsste dann über ein Auskunftsersuchen entscheiden (§ 480 Abs. 1 Satz 1 StPO) – unter Anwendung der sehr restriktiven Auskunftsregelungen der Strafprozessordnung (§ 474 Abs. 2 StPO).

Der Evaluationsbericht zeigt jedoch zugleich überzeugend auf, dass § 24c Abs. 7 Satz 4 Nr. 3 ASOG 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 aus Sicht des Weizenbaum-Instituts in der Begründung zum Gesetzentwurf klarstellen, dass § 24c Abs. 7 S. 4 Nr. 1 ASOG keine Sperrwirkung gegenüber § 24c Abs. 7 S. 4 Nr. 3 ASOG entfaltet.

24c Abs. 2, 5 und 8 ASOG konkretisieren insbesondere die Möglichkeit, Body-Cams auch in nicht öffentlich zugänglichen Orten einzusetzen, wenn tatsächliche Anhaltspunkte für die Entstehung einer Gefahr für Leib, Leben oder Freiheit einer Person vorliegen und die Maßnahme zur Abwehr dieser Gefahr erforderlich erscheint.[14] Nach der bisherigen Fassung des § 24c ASOG[15] war der Einsatz in nicht-öffentlichen Räumen nur zulässig, sofern bereits eine

[13] Vgl. § 24c Abs. 7 S. 4 Nr. 3 ASOG.

[14] Vgl. § 24c Abs. 1 ASOG.

[15] § 24a ASOG Bln, vom 11.10.2006, gültig ab 09.08.2006 bis 23.12.2025.

Gefahr für Leib, Leben oder Freiheit bestand. Die Neuregelung führt damit zu einer Vorverlagerung der Eingriffsschwelle in das Gefahrenvorfeld.[16]

Die Entscheidung darüber, ob tatsächliche Anhaltspunkte für die Entstehung einer Gefahr vorliegen, obliegt den handelnden Polizeibeamt:innen im Vorfeld des Einsatzes. Dies ist einerseits mit erheblichen Einschätzungsschwierigkeiten verbunden und birgt andererseits die Gefahr gewichtiger Grundrechtseingriffe bereits auf Grundlage prognostischer Annahmen. Denn die dynamischen Einsatzsituationen, in denen Body-Cams benutzt werden, erstrecken sich regelmäßig nur über einen kurzen Zeitraum. Eine praktisch handhabbare Abgrenzung ist daher kaum zu leisten.[17] Für die Einsatzkräfte ist diese Differenzierung zwischen der konkreten Gefahr und der sog. konkretisierten Gefahr daher mit erheblichen Herausforderungen und Unsicherheiten verbunden. Der Wortlaut der Norm stellt auf die Differenzierung und die subjektive Wahrnehmung vor Ort durch die Beamt:innen ab. Dies wird deutlich an dem geänderten Wortlaut in der Novelle. Während der bisherige § 24c Abs. 2 i.V.m. Abs. 1 ASOG gesetzlich regelte, dass ein Body-Cam-Einsatz *„erforderlich ist"*[18]*, stellt der novellierte § 24c Abs. 1 Nr. 2 darauf ab, dass die Maßnahme „erforderlich erscheint"*. Diese novellierte Regelung hat insbesondere Folgen für die Betroffenen der Maßnahme in der nachträglichen gerichtlichen Überprüfung. Die Polizeibeamt:innen können nun entsprechend dem Wortlaut der Norm subjektiv vortragen, dass in ihrer Wahrnehmung, die Maßnahme zum Zeitpunkt ihrer Entscheidung über das „Ob" des Body-Cam-Einsatzes erforderlich *erschien*.

Die vorgesehene Regelung wirft verfassungsrechtliche Bedenken im Hinblick auf die Unverletzlichkeit der Wohnung (Art. 13 GG) sowie das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) auf. Der Schutz des Wohnraums zählt zu den besonders intensiv geschützten Grundrechten und darf nur unter strengen Voraussetzungen eingeschränkt werden. Soweit der Einsatz von Body-Cams Wohnungen betrifft, ist Art. 13 GG einschlägig; bei sonstigen nicht-öffentlichen Räumen ist jedenfalls das allgemeine Persönlichkeitsrecht berührt. Die Neufassung des ASOG versäumt es, die tatbestandlichen Voraussetzungen für den Einsatz von Body-Cams in nicht-öffentlichen Räumen hinreichend klar und eng zu begrenzen.

Zudem sieht die Novelle keine unabhängige Kontrolle oder systematische nachträgliche Überprüfung der Einsätze vor. Weder eine datenschutzrechtlich belastbare Protokollierung noch technische Schutzmaßnahmen zur Verhinderung einer Zweckentfremdung der Aufzeichnungen sind normiert. Damit fehlen zentrale rechtsstaatliche Sicherungen, die nach der Rechtsprechung des Bundesverfassungsgerichts bei besonders eingriffsintensiven Maßnahmen regelmäßig erforderlich sind.[19]

---

[16] So spezifisch für Bodycams: Landtag Schleswig-Holstein Drs. 20/988, S. 8. Allgemein zur Formulierung „wenn Tatsachen die Annahme rechtfertigen" Graulich, in: Lisken/Denninger, PolR-Hdb, 7. Aufl. 2021, Kap. E, Rn. 134.

[17] Ebenso für NRW, Arzt, in: BeckOK POR NRW, § 15c PolG NRW, Rn. 24.

[18] Vgl. § 24c ASOG Bln, vom 20.12.2023, gültig ab 24.12.2023 bis 23.12.2025.

[19] BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09, 1 BvR 1140/09 – BKAG.

In der Gesetzesbegründung heißt es, *„erforderlich, aber auch ausreichend als Voraussetzung für die Anfertigung von Bild- und Tonaufnahmen und -aufzeichnungen [sei] eine wenigstens hinreichend konkretisierte Gefahr für Leib, Leben oder Freiheit“*. Weiter wird ausgeführt, der Rechtsprechung des Bundesverfassungsgerichts[20] folgend müssten tatsächliche Anhaltspunkte für die Entstehung einer konkreten Gefahr vorliegen. Der zitierten BVerfG-Entscheidung[21] lag die verfassungsrechtliche Prüfung besonders weitreichender Befugnisse zur Abwehr des internationalen Terrorismus zugrunde. Das Bundesverfassungsgericht hat hierbei betont, dass tief in das Privatleben eingreifende Maßnahmen nur zum Schutz hinreichend gewichtiger Rechtsgüter zulässig sind, eine konkret absehbare Gefährdung voraussetzen und mit besonderen Vorkehrungen zum Schutz des Kernbereichs privater Lebensgestaltung, mit Transparenz-, Kontroll- und Löschungspflichten flankiert werden müssen.[22] Diese Anforderungen unterstreichen insbesondere die Bedeutung verfahrensrechtlicher Sicherungen, die im vorliegenden Gesetzentwurf aus Sicht des Weizenbaum-Instituts nicht in vergleichbarer Weise vorgesehen sind.

In § 24c Abs. 8 Satz 2 ASOG wird der Prüfungsmaßstab für die gerichtliche Entscheidung über die Nutzung der Bild- und Tonaufzeichnungen präzisiert. Der Gesetzesbegründung entsprechend hat das Gericht künftig die *Rechtmäßigkeit der bereits erfolgten Datenerhebung* zu prüfen, nicht mehr die Rechtmäßigkeit der beabsichtigten Datennutzung. Auch wenn diese zeitliche Verlagerung der gerichtlichen Kontrolle angesichts von Art. 13 Abs. 5 Satz 2 GG nicht per se verfassungswidrig ist, erscheint es aus rechtsstaatlicher Perspektive geboten, eine vorgelagerte gerichtliche Kontrolle der Datennutzung weiterhin vorzusehen. Andernfalls drohen einschneidende Grundrechtseingriffe, deren Rechtmäßigkeit erst nachträglich überprüft werden kann, obwohl eine einmal erfolgte Verletzung der betroffenen Grundrechte nicht rückgängig zu machen ist. Bereits der Evaluationsbericht[23] empfahl eine gesetzliche Klarstellung, dass auch die Rechtmäßigkeit der Erhebung gerichtlich zu überprüfen ist.

Darüber hinaus werden die Grundrechte unbeteiligter Dritter in der Gesetzesbegründung nicht hinreichend berücksichtigt. Es bleibt unklar, wie mit Aufnahmen von grundsätzlich nicht betroffenen Personen im Hinblick auf Löschung und mögliche zweckändernde Weiterverarbeitung umzugehen ist. Hier zeigt sich aus Sicht des Weizenbaum-Instituts eine Regelungslücke in der ASOG-Novelle. Die Zweckbindung in § 24c Abs. 8 Satz 1 i. V. m. § 24c Abs. 7 Satz 4 ASOG schließt die Anwendbarkeit der §§ 42c und 42d ASOG nicht aus. Hierdurch bleibt eine Nutzung der Aufnahmen auch über die Speicherfristen hinaus, etwa zu anderen Zwecken, wie dem Training automatisierter KI-Systeme, möglich.[24] Das Bundesverfassungsgericht leitet aus dem nach Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG garantierten Recht auf

[20] BVerfG, Urteil vom 20. April 2016, 1 BvR 966/09, 1 BvR 1140/09 – BKAG.

[21] Ebd.

[22] Ebd.

[23] Margies/Hansel/von Steinsdorff/Kaiser/Blokland, Evaluation der Anwendung und Auswirkungen des §24c Allgemeines Sicherheits- und Ordnungsgesetz, Oktober 2024.

[24] Botta, Stellungnahme zum Entwurf eines Gesetzes zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin vom 26.09.2025, S.7.

informationelle Selbstbestimmung das Gebot der Normenklarheit ab, das der Vorhersehbarkeit von Eingriffen für die Bürger:innen, einer wirksamen Begrenzung der Befugnisse sowie der Ermöglichung einer effektiven Kontrolle durch die Gerichte dient. Daneben ergibt sich zumindest aus dem in Art. 20 Abs. 3 GG verankerten Rechtsstaatsgebot der allgemeine Bestimmtheitsgrundsatz.[25] Gerade vor diesem Hintergrund bedarf aus Sicht des Weizenbaum-Instituts klarerer gesetzlicher Grenzen.

Besonders kritisch ist schließlich die ersatzlose Streichung des bisherigen § 24c Abs. 10 ASOG zu bewerten, der eine unabhängige wissenschaftliche Evaluierung der Anwendung und Auswirkungen der Body-Cam-Nutzung vorsah. Der Evaluationsbericht wurde dem Abgeordnetenhaus vorgelegt und trug damit zur demokratischen Legitimation und evidenzbasierten Fortentwicklung der Norm bei. Eine vergleichbare Evaluierungspflicht enthält der § 24c ASOG nicht mehr. Die Berliner Beauftragte für Datenschutz und Informationsfreiheit kritisierte die Streichung von Evaluierungspflichten in sicherheitsrechtlichen Vorschriften als grundrechtlich problematisch.[26] Dieser Beurteilung schließt sich das Weizenbaum-Institut an. Evaluationen stellen kein bloßes formales Element dar, sondern sind ein wesentliches Instrument des Grundrechtsschutzes und einer evidenzbasierten Gesetzgebung.

Schließlich empfiehlt auch der Evaluationsbericht „Bodycams bei der Polizei Berlin“, den Einsatz von Body-Cams beim Rettungsdienst der Berliner Feuerwehr kritisch zu überprüfen.[27] Anders als bei der Polizei befürchten die Einsatzkräfte hier einen Vertrauensverlust bei Betroffenen. Weshalb der Gesetzgeber, der sich in vielen Punkten ausdrücklich auf den Evaluationsbericht stützt, an dieser Stelle davon abweicht, bleibt unbegründet.

Die vollständige Streichung der spezifischen Evaluierungspflicht in § 24c ASOG ist aus Sicht des Weizenbaum-Instituts insbesondere vor dem Hintergrund sich sehr schnell entwickelnder Technik und Technologien kritisch im Rahmen der Verhältnismäßigkeitsprüfung zu betrachten.

- Das Weizenbaum-Institut empfiehlt daher, eine gesetzliche Pflicht zur unabhängigen wissenschaftlichen Evaluierung der Nutzung von Body-Cams in nicht-öffentlichen Bereichen vorzusehen und den Einsatz von Body-Cams bei Feuerwehr- und Rettungsdiensten auszuschließen.

- Aus Sicht des Weizenbaum-Instituts erscheint es geboten, um eine verhältnismäßige Ausgestaltung zu gewährleisten, den Einsatz von Body-Cams in nicht-öffentlichen Räumen auf konkrete, dokumentierte Gefahrenlagen zur Abwehr erheblicher Gefahren, die ein polizeiliches Einschreiten erfordern, zu beschränken.

[25] Eichberger, in: Huber/Voßkuhle, GG, Bd. I, 8. Aufl. 2024, Art. 2 Abs. 1, Rn. 294 f.

[26] Berliner Beauftragte für Datenschutz und Informationsfreiheit, Stellungnahme zum Fünfundzwanzigsten Gesetz zur Änderung des Allgemeinen Sicherheits- und Ordnungsgesetzes (Drucksache 19/2265) v. 06. März 2025; zu §§ 25b, 25c ASOG.

[27] Margies/Hansel/von Steinsdorff/Kaiser/Blokland, Evaluation der Anwendung und Auswirkungen des §24c Allgemeines Sicherheits- und Ordnungsgesetz, Oktober 2024.

\\ Das Weizenbaum-Institut empfiehlt außerdem, gesetzliche Vorgaben zur umfassenden Protokollierung, zur nachträglichen Kontrolle sowie zu technischen Sicherungen gegen Zweckentfremdung ausdrücklich festzuschreiben.

# 4 Videoüberwachung an kriminalitätsbelasteten Orten und automatisierte Verhaltensanalyse (§ 24e ASOG)

Die Einführung einer erweiterten Videoüberwachung an kriminalitätsbelasteten Orten,[28] verbunden mit der Möglichkeit einer automatisierten Auswertung von Verhaltensmustern, stellt einen qualitativen Sprung in der polizeilichen Überwachung dar. Die Norm begründet mehrere eigenständige Eingriffe in das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG, die jeweils gesondert am Maßstab der Verhältnismäßigkeit zu messen sind.

Maßgeblich ist insoweit vorrangig die Rechtsprechung des Bundesverfassungsgerichts zum Recht auf informationelle Selbstbestimmung, insbesondere zu automatisierten Datenanalysen und zur Generierung grundrechtsrelevanten „neuen Wissens". Die JI-RL[29] und die KI-VO grenzen zwar den Handlungsrahmen der Mitgliedstaaten ein. Die Richtlinie belässt den Mitgliedstaaten jedoch substanzielle Regelungsspielräume, von denen die landesrechtlichen Regelungen Gebrauch machen. Auch die KI-VO determiniert den polizeilichen Einsatz von KI-Systemen als produktsicherheitsrechtliche Vorgabe (mit Ausnahmen wie den Verbotsregelungen des Art. 5 KI-VO) nicht vollständig.

Ob § 24e ASOG den grundrechtlichen Anforderungen genügt, bestimmt sich vorrangig nach den Vorgaben des Grundgesetzes, nicht der Grundrechtecharta der EU.[30]

Eine automatisierte Datenanalyse stellt zusätzlich zur ursprünglichen Datenerhebung einen Eingriff in das Recht auf informationelle Selbstbestimmung aller Personen dar, deren Daten bei diesem Vorgang personenbezogen Verwendung finden.[31]

Dieser Grundrechtseingriff muss verhältnismäßig, insbesondere angemessen sein. Außerdem muss er sich verfassungsrechtlich nach dem Grundsatz der Zweckbindung

[28] Vgl. § 17a ASOG.

[29] RICHTLINIE (EU) 2016/680 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates.

[30] Vgl. BVerfGE 152, 152 (169).

[31] BVerfGE 165, 363 (388).

rechtfertigen lassen.[32] Ein Grundrechtseingriff erwächst zudem nicht nur aus der Datenzusammenführung, sondern darüber hinaus daraus, dass die automatisierte Datenanalyse nach § 24e Abs. 4 ASOG grundrechtsrelevantes neues Wissen generiert.[33] Die automatisierte Auswertung der erhobenen Bilddaten stellt einen eigenständigen, gegenüber der bloßen Erhebung und Speicherung qualitativ neuen Grundrechtseingriff dar. Sie erschöpft sich nicht in einer zweckwahrenden Weiternutzung vorhandener Daten, sondern ist auf die algorithmische Generierung neuer, grundrechtsrelevanter Erkenntnisse gerichtet. Diese Weiterverarbeitung kann spezifische Belastungen mit sich bringen.[34]

Der Gesetzgeber versucht, diese Intensivierung durch mehrere Begrenzungen abzumildern: Ein automatisiertes Auslösen behördlicher Maßnahmen ist ausgeschlossen, ebenso die biometrische Fernidentifizierung. Laut der Gesetzesbegründung ist außerdem „*die automatisierte Mustererkennung lediglich dazu gedacht, jene Polizeivollzugsbeamtinnen und -beamten, die die Bildschirme betrachten, bei der Auswertung zu unterstützen. Es handelt sich hier um ein Assistenzsystem.*“ Angesichts der technischen Komplexität, der geringen Transparenz und der potenziellen Erfassung Unbeteiligter reicht diese Einschränkung jedoch aus Sicht des Weizenbaum-Instituts nicht aus, um die Grundrechtsbelastung zu minimieren.

Dem in § 24e ASOG genannten Schutzzweck (Straftaten allgemein sowie Unglücksfälle i. S. d. § 323c Abs. 1 StGB) steht eine verdachtsunabhängige, flächendeckende Auswertung gegenüber. Der Ausschluss autonomer Entscheidungen verlagert die Eingriffsentscheidung zwar formal zurück auf den Menschen, ändert aber nichts daran, dass die algorithmische Vorauswahl den Wahrnehmungs- und Entscheidungsspielraum der Beamt:innen faktisch beeinflussen kann.

Zu begrüßen ist aus Sicht des Weizenbaum-Instituts, dass in § 24e Abs. 4 ASOG die Anpassungen aus dem Änderungsantrag übernommen wurden und die Nutzung der Bildaufnahmen für das Testen oder Trainieren biometrischer Systeme nun ausdrücklich ausschließt. Darüber hinaus dürfen Maßnahmen gegen einzelne Personen erst nach Sichtung der Bildaufnahmen oder der Inaugenscheinnahme der Lage vor Ort erfolgen.

Im Rahmen der Verhältnismäßigkeit ist jedoch bereits die Frage der Geeignetheit, zumindest aber der Erforderlichkeit kritisch zu bewerten. Zahlreiche Studien haben belegt, dass (konventionelle) Videoüberwachung in der Regel kein effektives Mittel für die Reduktion von Kriminalität darstellt.[35] Vor allem bei Gewalt gegen Personen sind keine oder bestenfalls geringe Effekte nachweisbar. Um erfolgreich Gewalt gegen Personen zu verhindern, müssen Einsatzkräfte nicht nur mithilfe des Assistenzsystems informiert werden, sondern auch ausreichend schnell vor Ort sein. In der Novelle des ASOG fehlt aus Sicht des Weizenbaum-

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

[33] BVerfGE 165, 363 (388 f.); Kurt Graulich, Elemente eines Polizeiverfassungsrechts, NVwZ-Beilage 2023, 27 (30); Dieter Kugelmann/Antonia Buchmann, Der Algorithmus und die Künstliche Intelligenz als Ermittler, GSZ 2024, 1 (5); vgl. BVerfGE 156, 11 (39 f.).

[34] BVerfGE 165, 363 (390); Bäuerle (Fn. 42), ZD 2025, 128 (130).

[35] Kammerer, Dietmar (2008): Bilder der Überwachung. Frankfurt/Main, S. 76-83.

Instituts ein Konzept zur Umsetzung einer „Echtzeitintervention“ und zu den zusätzlichen Personalkosten, die hier dauerhaft entstehen.[36]

Zur Wirkung von KI-gestützter Verhaltensanalyse zum Zweck der Kriminalprävention liegen noch keine ausreichenden unabhängig und wissenschaftlich erhobenen Erkenntnisse vor.[37] Es ist davon auszugehen, dass in Berlin ein System zum Einsatz kommen kann, das zu Pilotversuchen in Mannheim und in Hamburg vergleichbar ist.[38] Das Folgende referiert Erfahrungen aus diesen Einsätzen.[39]

Die Stadt Mannheim betreibt seit 2018 das Pilotprojekt „Intelligente Videoüberwachung“ in einer Projektpartnerschaft mit dem Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung (IOSB). Weil die ursprünglichen Projektziele nach fünf Jahren nicht erreicht wurden, wurde die Laufzeit verlängert. Mit Stand von März 2025 ist die in Mannheim eingesetzte KI weiterhin im Stadium der Entwicklung. Die von ihr generierten Alarme „*werden für die Weiterentwicklung des Systems ausgewertet und dienen der Analyse sowie Optimierung von Schwachstellen*“[40], sind also nicht Teil der polizeilichen Praxis.

In Hamburg hat ein Modellprojekt am Hansaplatz zu zahlreichen Fehlalarmen geführt. Das Projekt endet nach derzeitiger Planung am 31.08.2026 mit einer umfassenden Evaluation, die Aufschluss darüber geben soll, in welchem Maße das Assistenzsystem eine Unterstützung der polizeilichen Aufgabenwahrnehmung darstellt und wie nachvollziehbar sich die Meldungen für die Videobeobachter:innen darstellen. Von 1.140 Hinweisen durch das System im Zeitraum von zwei Monaten wurden bisher lediglich elf als polizeilich relevant eingestuft.[41] Die Software war nicht imstande, zuverlässig Gesten und Bewegungen voneinander abzugrenzen (etwa Schläge von einer Umarmung).[42] Um die Erkennungsrate zu verbessern, sieht § 42d ASOG die Erlaubnis vor, KI-Systeme zu trainieren. Hierdurch kann ein Druck zur Ausweitung der KI-gestützten Videoüberwachung auf weitere Standorte allein aufgrund der technischen Notwendigkeit entstehen und nicht aus polizeitaktischen Erwägungen.

Vor diesem Hintergrund einer offenbar hohen Zahl an Fehlalarmen (*false positive rate*) bei dieser Technologie ist es zwar zu begrüßen, dass das System keine autonomen Entscheidungen treffen darf, sondern lediglich als „Assistenzsystem“ fungieren soll (§ 24e Abs. 4 ASOG). Allerdings besteht die Gefahr, dass auch gut eingestellte „Assistenzsysteme“ in der Praxis den Spielraum möglicher Handlungen der Beamt:innen so weit einschränken, dass eine

---

[36] Eine solche „Echtzeitintervention“ ist erklärtes Ziel der Mannheimer Polizei. Vgl. Landtag von Baden-Württemberg. (2022). *Auswertung des Projektes „Intelligente Videoüberwachung“ in Mannheim* (Drucksache 17/2833).

[37] Vgl. Lang, J. (2023). Intelligente Videoüberwachung. Eine Wirkungsanalyse am Beispiel der Verhaltens-/Bewegungsmustererkennung. *Kriminalistik*, *2*, 124–128.

[38] Golda, T., Cormier, M., & Beyerer, J. (2023). Intelligente Bild- und Videoauswertung für die Sicherheit. In D. Wehe & H. Siller (Hrsg.), *Handbuch Polizeimanagement* (S. 1487–1507). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-34388-0_87.

[39] Vgl. Drucksachen des Landtags Baden-Württemberg 17/2833, 17/5816, 17/8478, 17/8545; Drucksachen der Hamburgischen Bürgerschaft 22/12180, 22/12339, 22/12356, 22/12984, 22/13988, 22/14472, 22/17455.

[40] Drucksache 17/8545, S. 2, Hamburg.

[41] Drucksache 22/17455, S. 4, Hamburg.

[42] Drucksache 22/12339, S. 3, Hamburg.

„Unterstützung" von einer „Entscheidung" nicht mehr zu unterscheiden ist. In der Gesetzesbegründung fehlt es aus Sicht des Weizenbaum-Instituts an Erläuterungen, die darstellen, wie die Beamt:innen geschult werden sollen. Zudem sind Dokumentationspflichten zu empfehlen, damit für die Betroffenen einer polizeilichen Maßnahme nachvollziehbar ist, wie es zu der Entscheidung gekommen ist.

Kriminalitätsbelastete Orte sind außerdem seit jeher diskriminierungsanfällig. Anlassunabhängige Maßnahmen erhöhen das Risiko, dass polizeiliches Ermessen an sozial zugeschriebene Merkmale anknüpft. Automatisierte Systeme können dieses Risiko einerseits mindern, indem sie menschliche Stereotype ersetzen; andererseits bringen sie eigene Diskriminierungspotentiale mit sich. Insbesondere Verhaltensmuster von marginalisierten Personen, wie etwa bei Behinderungen oder Wohnungslosigkeit, können algorithmisch als „auffällig" klassifiziert werden und zu mehrfach Diskriminierungen führen.[43]

Das Bundesverfassungsgericht hat hervorgehoben, dass Diskriminierungsrisiken automatisierter Systeme umso weniger hinnehmbar sind, je näher ihre Wirkungen an eine nach Art. 3 Abs. 3 GG unzulässige Benachteiligung heranreichen. Zwar enthalten §§ 42d und 47a ASOG deklatorische Diskriminierungsverbote, doch bleiben zentrale Fragen ungeregelt. Damit werden wesentliche Entscheidungen in die Verwaltungspraxis verlagert.[44]

Der neu eingeführte § 12 Abs. 3 ASOG vermag diese Defizite aus Sicht des Weizenbaum-Instituts nicht aufzufangen. Als einfachgesetzliche Konkretisierung bleibt er hinter dem verfassungsrechtlichen Anknüpfungsverbot des Art. 3 Abs. 3 GG zurück und entfaltet überwiegend deklaratorische Wirkung. Eine präzisere gesetzgeberische Steuerung hätte nicht nur die Rechtssicherheit für die Praxis erhöht, sondern zugleich zur Reduktion der informationellen Eingriffsintensität beitragen können.[45]

Es ist aus Sicht des Weizenbaum-Instituts jedoch unerlässlich gesetzlich klarzustellen, dass auch die in Berlin eingesetzte Hardware nicht nur technische Anforderungen erfüllt, sondern auch ethischen, rechtlichen und sicherheitspolitischen Maßstäben genügt und dies gesetzlich verankert wird.

Die Anpassungen, die durch den Änderungsantrag in die Novelle aufgenommen wurden, adressieren nicht die potenziellen Verzerrungen der KI-Systeme, die marginalisierte Gruppen überproportional erfassen können, noch die hohe Zahl an Fehlalarmen, die Pilotprojekte in Mannheim und Hamburg gezeigt haben. Zudem werden ethische und sicherheitstechnische Fragen zur eingesetzten Hardware nicht geregelt.

\\ Vor diesem Hintergrund empfiehlt das Weizenbaum-Institut, die automatisierte Verhaltensanalyse gesetzlich auf die Abwehr konkreter Gefahren für besonders gewichtige Rechtsgüter (Leib, Leben, Freiheit) zu beschränken. Außerdem sollte der

---

[43] Sußner, *Try harder hilft selten: Eine verfassungsrechtliche Einordnung der Videoüberwachung an kriminalitätsbelasteten Orten, VerfBlog,* 2026/1/08, https://verfassungsblog.de/berlin-asog-novelle-kbos/, DOI: 10.59704/7bd1f58e3170253a.

[44] Ebd.

[45] Ebd.

Einsatz konkreten Dokumentationspflichten unterliegen, die insbesondere die Entscheidung für Betroffene polizeilicher Maßnahmen nachprüfbar macht. Zu begrüßen wären zudem, striktere Zweckbindungs- und Nutzungsbeschränkungen, um eine nachträgliche Zweckentfremdung der erhobenen Daten auszuschließen, insbesondere für das Testen oder Trainieren von KI-Systemen.

- Darüber hinaus empfiehlt das Weizenbaum-Institut verbindliche Vorgaben zum Diskriminierungsschutz und zur Systemgestaltung, die über § 12 Abs. 3 ASOG hinausgehen: Es sollten regelmäßige externe Audits, die Offenlegung von Trainingsdaten und Algorithmen, soweit datenschutzrechtlich und geheimnisschutzrechtlich zulässig sowie klare Verantwortlichkeiten für Fehlalarme und Diskriminierungseffekte vorgeschrieben werden. Ebenfalls geboten erscheint die gesetzliche Festlegung technischer Mindeststandards und Sicherheitsanforderungen an eingesetzte Hard- und Software, um ethische, informationelle und geopolitische Risiken zu minimieren.
- Außerdem ist die Wiedereinführung einer unabhängigen wissenschaftlichen Evaluation aus Sicht des Weizenbaum-Instituts zu empfehlen, verbunden mit regelmäßiger Berichterstattung an das Abgeordnetenhaus. Ergänzend sollte gesetzlich verankert werden, dass die Fortgeltung der Befugnisse an einen positiven Evaluationsbefund gekoppelt ist. Schließlich sind parlamentarische Kontrollrechte und öffentliche Transparenz durch jährliche Berichte über Einsatzorte, Dauer, Fehlalarmquoten und polizeiliches Einschreiten zu stärken.

# 5 Nachträglicher biometrischer Abgleich mit öffentlich zugänglichen Daten aus dem Internet (§ 28a ASOG)

Aus interdisziplinärer Perspektive wirft der neu geschaffene § 28a ASOG erhebliche verfassungs-, unions- und gesellschaftsrechtliche Bedenken auf. Die vorgesehene Möglichkeit, biometrische Gesichts- und Stimmmerkmale mit öffentlich zugänglichen Internetdaten abzugleichen (sog. „Data Scraping“), läuft faktisch auf den Aufbau umfassender biometrischer Referenzbestände hinaus, da ein Abgleich ohne vorgelagerte Datenextraktion technisch kaum realisierbar ist. Ein solches Auslesen, das zahlreiche unbeteiligte Personen erfassen wird, wirft aus Sicht des Weizenbaum-Instituts sowohl nach Art. 5 Abs. 1 lit. e KI-VO europarechtliche als auch nach dem Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) verfassungsrechtliche Bedenken auf.

Nach Art. 5 Abs. 1 lit. e KI-VO zählen zu den verbotenen Praktiken im KI-Bereich das Inverkehrbringen, die Inbetriebnahme oder die Verwendung von KI-Systemen, die Datenbanken zur Gesichtserkennung durch das ungezielte Auslesen von Gesichtsbildern aus dem Internet oder von Überwachungsaufnahmen erstellen oder erweitern.

Biometrische Daten zählen nach der Rechtsprechung des BVerfG[46] zu den besonders sensiblen Persönlichkeitsmerkmalen, weil sie einzigartige körperliche Merkmale erfassen. Zudem werden nicht nur Zielpersonen, sondern auch zahlreiche unbeteiligte Personen erfasst, da alle öffentlich zugänglichen Bilder aus dem Internet als Referenzdaten dienen können.[47] Ihre massenhafte Erhebung zu Referenzzwecken birgt erhebliche Missbrauchsgefahren und Machtasymmetrien.

Unabhängig von der Frage des Datenbankaufbaus bleibt auch der einzelne Abgleich hoch eingriffsintensiv. Wegen der strukturell unbegrenzten Streubreite und der Möglichkeit, Rückschlüsse auf sensible Lebensbereiche zu ziehen sowie der bekannten Fehler- und Diskriminierungsrisiken biometrischer Systeme entsteht ein gravierendes Gefährdungspotenzial für Grundrechte und gesellschaftliche Teilhabe.[48] Diese Eingriffstiefe ist mit erheblichen *chilling effects* auf das allgemeine Persönlichkeitsrecht, die Meinungs- und Versammlungsfreiheit und anderen erheblichen Verhaltensanpassungen verbunden.[49] Die KI-gestützte Auswertung verstärkt die Eingriffsintensität und birgt zusätzliche Risiken durch Automatisierung, Fehleranfälligkeit und mögliche (Mehrfach-)Diskriminierung.

Zudem bleibt im Gesetzestext weitgehend auslegungsbedürftig, welche Art von *„Abgleich"* gemeint ist. Ohne präzise Festlegung der möglichen Maßnahmen, die unter *„Abgleich"* zu subsumieren sind, wie unter anderem Identifizierung, Rasterfahndung oder Profilbildung, die jeweils unterschiedlich zu bewertende Eingriffsintensitäten aufweisen, ist eine datenschutzrechtliche Verhältnismäßigkeitsprüfung kaum möglich. Auch das verfassungsrechtliche Bestimmtheitsangebot ist aufgrund der Auslegungsschwierigkeiten gefährdet.[50] Zu betonen ist aus Sicht des Weizenbaum-Instituts die Fehleranfälligkeit der entsprechenden KI-Auswertungssysteme.[51] Selbst geringe Fehlerraten führen bei einem Masseneinsatz zu vielen Fehltreffern. Empirisch bestehen höhere Fehlerraten bei marginalisierten Personengruppen, was das mehrfache Diskriminierungsrisiko erhöht.[52]

Durch den Verweis auf § 42a Abs. 3 ASOG können außerdem hochsensible Daten aus verdeckten Maßnahmen genutzt werden, auch wenn die jeweilige Gefahrenschwelle im Sinne

---

[46] BVerfG, Beschluss vom 18. Dezember 2018, 1 BvR 142/15, Rn. 53: „höchstpersönliche Merkmale wie das Gesicht"; vgl. auch BVerfG, Urteile des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19 und 1 BvR 2634/20, Rn. 87.

[47] Vgl. Wortlaut des § 28a Abs. 1 „(...) biometrisch mit allgemein öffentlich zugänglichen personenbezogenen Daten aus dem Internet abgleichen".

[48] Vgl. Hunold, Aden, Thurn, Berger, Ohder, Sticher, Strauß; Polizei und Diskriminierung, Risiken Forschungslücken, Handlungsempfehlungen.

[49] Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI), Stellungnahme der Berliner Beauftragten für Datenschutz und Informationsfreiheit zum Gesetzentwurf zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, Ausführungen zu § 28a ASOG ab S.11.

[50] Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI), Stellungnahme der Berliner Beauftragten für Datenschutz und Informationsfreiheit zum Gesetzentwurf zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, Ausführungen zu § 28a ASOG ab S.11.

[51] Vgl. Ausführungen weiter oben.

[52] Ogorek, LTZ 2004, 274 (280), unter Verweis auf Grother/Ngan/Hanaoka (NIST), Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, Dezember 2019, S.2.

von § 25b Abs. 1 S. 1 ASOG beziehungsweise § 26b Abs. 1 ASOG in Verbindung mit § 26a Abs. 1 ASOG erreicht worden sein muss. Dies verschärft den Eingriff zusätzlich und zeigt, wie weitreichend die Ermächtigungsgrundlage angelegt ist. Die vorgesehenen Kontrollmechanismen sehen unter anderem vor, dass intern Datenschutzbeauftragte informiert werden; eine unabhängige und regelmäßige Kontrolle ist gesetzlich hingegen nicht vorgesehen.[53] Auch fehlen Benachrichtigungspflichten für Betroffene, was ein erhebliches Rechtsschutzdefizit für diese bedeutet.

Durch den Änderungsantrag wurde der § 28a ASOG zudem erweitert, indem der Anwendungsbereich auf Kontakt- und Begleitpersonen ausgeweitet worden ist. Die Polizei kann biometrische Daten zu Gesichtern und Stimmen nicht nur der in den in § 28a Abs. 1 S. 1 Nr. 1-3 ASOG genannten Personen, sondern auch deren Kontakt- und Begleitpersonen mittels automatisierter Anwendungen zur Datenverarbeitung zum Zweck der Identifizierung und der Ermittlung des Aufenthaltsortes biometrisch mit öffentlich zugänglichen Daten aus dem Internet abgleichen. Wer eine Kontakt- oder Begleitperson ist, ist legaldefiniert in § 18 Abs. 2 Nr. 1 Buchstabe b ASOG. Eine Kontakt- oder Begleitperson ist hiernach eine Person, die *„mit einer in (§ 18 Abs. 2 Nr. 1) Buchstabe a (ASOG) genannten Person nicht nur in einem flüchtigen oder zufälligen Kontakt, sondern in einer Weise in Verbindung steht, die die Erhebung ihrer personenbezogenen Daten zur vorbeugenden Bekämpfung solcher Straftaten erfordert; dies ist der Fall, wenn Tatsachen die Annahme einer individuellen Nähe der Person zu solchen Straftaten rechtfertigen, insbesondere weil eine in Buchstabe a genannte Person sich dieser Person zur Begehung der Straftaten bedienen könnte oder die Person von der Planung oder Vorbereitung der Straftaten Kenntnis hat oder daran mitwirkt (Kontakt- und Begleitperson).“* Der biometrische Abgleich mit öffentlich zugänglichen Internetdaten stellt bereits für gefahrenverantwortliche Personen einen intensiven Eingriff in das Recht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG dar. Durch die Erweiterung auf Kontakt- und Begleitpersonen wird der Personenkreis der Maßnahme erhöht. Im Kontext der biometrischen Fernidentifizierung, die bereits aufgrund der Nutzung künstlicher Intelligenz und der Vielzahl durchsuchter Internetquellen eine hohe Eingriffsintensität aufweist, führt dies zu einer Potenzierung der Grundrechtsbeeinträchtigungen von Personen, die aus Sicht des Weizenbaum-Instituts problematisch im Sinne der Verhältnismäßigkeit ist.[54]

Die Anknüpfung an unbestimmte Begriffe, die für potenziell Betroffene unklare Begrenzung des Adressatenkreises sowie das Fehlen spezifischer Verfahrensschutzmechanismen, einschließlich solcher zum Diskriminierungsschutz und zur Wahrung des Kernbereichs privater Lebensgestaltung, verdeutlichen strukturelle Defizite der Novelle. Die automatische Löschpflicht und die Voraussetzung der menschlichen Aufsicht bei der KI-gesteuerten

[53] Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI); Stellungnahme der Berliner Beauftragten für Datenschutz und Informationsfreiheit zum Änderungsantrag der Fraktion der CDU und der Fraktion der SPD zur Drucksache 19/2553: Gesetz zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, S.2.

[54] Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI); Stellungnahme der Berliner Beauftragten für Datenschutz und Informationsfreiheit zum Änderungsantrag der Fraktion der CDU und der Fraktion der SPD zur Drucksache 19/2553: Gesetz zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, S.2.

Datenverarbeitung ist zwar positiv zu bewerten, jedoch reichen diese Verankerungen aus Sicht des Weizenbaum-Instituts nicht aus, um die verfassungs- und unionsrechtlichen Bedenken auszuräumen.

\\ Das Weizenbaum-Institut empfiehlt daher eine Streichung des § 28a ASOG.

# 6 Nutzung polizeilicher Datenbestände für KI-Systeme (§ 42d ASOG)

Die vorgesehene Nutzung polizeilicher Datenbestände zum Training und zur Testung automatisierter Verfahren wirft grundlegende unionsrechtliche und verfassungsrechtliche Fragen auf. Polizeidaten enthalten in der Regel personenbezogene Daten, deren Verwendung für KI-Systeme mit erheblichen Risiken verbunden ist.

Besonders gravierend ist die Gefahr, dass bestehende diskriminierende Strukturen in die eingesetzten Systeme übertragen werden. Historische Polizeidaten sind regelmäßig Ausdruck gesellschaftlicher Selektivitäten und spiegeln institutionelle Praktiken wider, die nicht frei von Diskriminierung sind. Werden solche Daten zur Modellbildung herangezogen, besteht das Risiko einer Verstärkung von Diskriminierungseffekten. KI-gestützte Analysesysteme können Verzerrungen aufweisen, die insbesondere marginalisierte Gruppen überproportional erfassen oder verdächtigen. Diese Form des Data Bias kann bestehende gesellschaftliche Ungleichheiten reproduzieren und verstärken.[55]

So fließen nicht nur personenbezogene Daten von Straftäter:innen oder Störer:innen, sondern auch von Geschädigten, Zeug:innen und Unbeteiligten in die Analyseplattformen ein. Diese Datenmengen zu präventiven Zwecken zusammenzuführen und auszuwerten, kann Persönlichkeitsprofile hervorbringen, die auch Diskriminierungen begünstigen.[56] Dies zeigt sich insbesondere an Anwendungen vorhersehender Polizeiarbeit (sogenanntes Predictive Policing). Die scheinbare Objektivität von algorithmischen Berechnungen täuscht schnell darüber hinweg, dass die Datengrundlagen und damit auch aus ihnen abgeleitete Vorhersagen nicht neutral sind. Rassistische Einstellungen und/oder klassistische Sichtweisen einzelner Polizeibeschäftigter kann polizeiliches Handeln in der analogen Welt beeinflussen und daher auch die Datenbasis für Predictive Policing verzerren.[57] Die bestehenden Risiken polizeilicher Datenanalyse potenzieren sich beim Einsatz künstlicher Intelligenz zusätzlich. Insbesondere bei lernfähigen Systemen bleibt der konkrete Prozess bis zur Ausgabe oftmals selbst für die Softwareentwickler intransparent (sogenanntes Blackbox Phänomen).[58] Dies

[55] BSI, Bias in der künstlichen Intelligenz, Whitepaper v. 24.07.2025, aufgerufen am 10.11.2025 unter url: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KI/Whitepaper_Bias_KI.pdf?__blob=publicationFile&v=5; ISO/IEC TR 24027. 2021. Bias in AI systems and AI aided decision making. Geneva: ISO/IEC, 2021.

[56] Martini/Botta, Polizeiliche Datenanalyse mittels KI, DÖV 2025

[57] Daniela Hunold/Hartmut Aden/Roman Thurn u.a., Polizei und Diskriminierung, 2025; Astrid Jacobsen/Jens Bergmann, Diskriminierungsrisiken in der Polizeiarbeit, 2024.

[58] Martini, Blackbox Algorithmus, 2019, S. 41 ff.

erschwert nicht nur die Nachvollziehbarkeit der Ergebnisse, sondern vor allem auch die Identifikation von Fehlern und Diskriminierungen.[59]

## 6.1 Vereinbarkeit mit Art. 5 Abs. 1 lit. c KI-VO

Die Verbote des Art. 5 KI-VO gelten seit dem 2. Februar 2025 (Art. 113 Abs. 3 lit. a KI-VO).

Art. 5 Abs. 1 lit. c KI-VO verbietet sogenanntes Social Scoring. Das Inverkehrbringen, die Inbetriebnahme oder die Verwendung von KI-Systemen zur Bewertung oder Einstufung von natürlichen Personen oder Gruppen von Personen über einen bestimmten Zeitraum auf der Grundlage ihres sozialen Verhaltens oder bekannter, abgeleiteter oder vorhergesagter persönlicher Eigenschaften oder Persönlichkeitsmerkmale kann danach untersagt sein. Hinzukommen muss eine Schlechterstellung oder Benachteiligung bestimmter natürlicher Personen oder Personengruppen. Aus Sicht des Weizenbaum-Instituts ist fraglich, ob schon das Trainieren oder Testen eines polizeilichen KI-Systems diese Voraussetzungen erfüllt. Sieht man schon in der Datenverarbeitung einzelner Personen eine individuelle Benachteiligung, dann wären die Voraussetzungen erfüllt.

Das Verbot greift aber nur, wenn eine von zwei weiteren alternativen Voraussetzungen erfüllt ist:

1. die Schlechterstellung steht in keinem Zusammenhang zu den Umständen, unter denen die Daten ursprünglich erzeugt oder erhoben wurden;

2. oder sie ist im Hinblick auf das soziale Verhalten oder dessen Tragweite ungerechtfertigt oder unverhältnismäßig.

Die erste Alternative ist eine Ausformung des Zweckbindungsgrundsatzes.[60] Die Weiterverarbeitung von personenbezogenen Daten könnte eine Verletzung dieser ersten Alternative darstellen. Fraglich ist jedoch, ob dieser strenge Zweckbindungsgrundsatz auch für Erlaubnistatbestände gilt, die unter Art. 4 Abs. 2 JI-Rl fallen, denn dieser sieht eine Ausnahme vom Zweckbindungsgrundsatz vor. Würde die KI-VO der JI-RL vorgehen, dann wäre die Ausnahme des Art. 4 Abs. 2 JI-RL nicht anwendbar. Nach Art. 2 Abs. 7 S. 2 KI-VO berührt die KI-VO jedoch nicht die JI-RL. Ausgenommen davon sind lediglich Art. 10 Abs. 5 KI-VO (die Regelung enthält einen zusätzlichen Ausnahmetatbestand für die Verarbeitung besonderer Kategorien personenbezogener Daten) und Art. 59 KI-VO (Weiterverarbeitung von personenbezogenen Daten innerhalb von KI-Reallaboren).[61]

Das Verbot des Art. 5 Abs. 1 lit. c alt. 1 KI-VO greift demnach nicht, wenn eine nationale Rechtsgrundlage besteht, die sich auf Art. 4 Abs. 2 JI-RL stützt. Genau eine solche könnte jedoch § 42d ASOG sein.

---

[59] Martini/Botta, Polizeiliche Datenanalyse mittels KI, DÖV 2025.

[60] Raue, in: BeckOK KI-Recht, 4. Ed. 1.11.2025, KI-VO, Art. 5 Rn. 63.

[61] Voigt, in: BeckOK KI-Recht, 4. Ed. 1.11.2025, KI-VO, Art. 2 Rn. 48.

Obwohl Art. 4 Abs. 2 EUV dem Unionsgesetzgeber für Bereiche der nationalen Sicherheit keine Regelungskompetenz einräumt, bleibt der Anwendungsbereich der JI-RL eröffnet, da polizeiliche KI-Trainingsmaßnahmen nicht den Schutz des Staates als solchen, mithin nicht die nationale Sicherheit, betreffen, sondern dem Bereich der öffentlichen Sicherheit zuzurechnen sind. Nach der Rechtsprechung des EuGH[62] fällt dieser Bereich in die unionsrechtliche Regelungszuständigkeit.[63] Der EuGH verlangt in diesem Zusammenhang, dass Einschränkungen datenschutzrechtlicher Garantien auf das absolut Notwendige begrenzt bleiben und gesetzliche Erlaubnistatbestände klare, berechenbare und verfahrensrechtlich abgesicherte Vorgaben enthalten.[64]

§ 42d ASOG könnte jedoch gegen Art. 5 Abs. 1 lit. c alt. 2 KI-VO verstoßen, wenn die Datenverarbeitung unverhältnismäßig ist.

## 6.2 Vereinbarkeit mit Art. 4 Abs. 1 lit. b iVm Art. 4 Abs. 2 JI-RL

Zentraler Prüfungsmaßstab ist der Grundsatz der Zweckbindung gemäß Art. 4 Abs. 1 lit. b JI-RL. Nach Art. 4 Abs. 1 lit. b JI-RL müssen personenbezogene Daten für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise verarbeitet werden. Polizei und Feuerwehr dürfen gemäß § 42d Abs. 1 S. 1 ASOG personenbezogene Daten auch mit einer Zweckänderung weiterverarbeiten. Eine Weiterverarbeitung zum Training und zur Testung KI-gestützter Systeme für Gefahrenabwehr- oder Einsatzaufgaben ist hiernach, soweit erforderlich, möglich. Dieser Erlaubnistatbestand müsste nach Art. 4 Abs. 2 lit. b JI-RL verhältnismäßig sein.

Nach § 42d Abs. 1 S. 2 und S. 3 ASOG ist bei der Weiterverarbeitung sicherzustellen, dass diskriminierende Algorithmen weder herausgebildet noch verwendet werden. Soweit wie technisch möglich, muss die Nachvollziehbarkeit des verwendeten Verfahrens sichergestellt werden. Personenbezogene Daten dürfen gemäß § 42d Abs. 1 S. 2 ASOG nicht zum Trainieren oder Testen von KI-Systemen weiterverarbeitet werden, wenn die Daten nicht mit Hilfe solcher KI-Systeme erhoben oder verarbeitet werden dürften.[65]

Trotz dieser gesetzlich verankerten Hinweise könnte die Regelung des § 42d S. 1 ASOG unverhältnismäßig sein.[66] Dies gilt insbesondere, da eine Verarbeitung von Daten (unbeteiligter) Dritter durch die Norm nicht ausgeschlossen ist. Soweit die Vorschrift gegen Art. 4 Abs. 1 lit. b i.V.m Art. 4 Abs. 2 JI-Rl verstößt, könnte auch ein Verstoß gegen Art. 5 Abs. 1 lit. c alt. 1 KI-VO vorliegen.

---

[62] EuGH, CR 2008, 381 (382).

[63] Martini/Botta: Polizeiliche Datenanalyse mittels KI, DÖV 2025, S. 1033, 1038.

[64] 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.

[65] Vgl. Änderungsantrag der Fraktion der CDU und der Fraktion der SPD zur Drucksache 19/2553, S. 13.

[66] Vgl. Botta, Stellungnahme zum Gesetz zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin (AGH-Drs. 19/2553), S. 7.

Darüber hinaus erlaubt § 42d Abs. 2 S. 2, 3 ASOG es den Behörden, auf Anonymisierung und Pseudonymisierung der Daten zu verzichten, wenn diese jeweils nur mit einem unverhältnismäßigen Aufwand möglich sind. In der Praxis ist jedoch eine wirksame Anonymisierung komplexer Datensätze, insbesondere bei biometrischen oder Verhaltensdaten, regelmäßig sehr aufwändig bis unmöglich. Die Regelung läuft daher auf eine systematische Verwendung von Klardaten hinaus. Im Bereich sicherheitsbehördlicher Datensammlungen besteht ein erhebliches Risiko, dass auch besonders schutzwürdige Informationen im Sinne von Art. 10 JI-RL in Trainingsprozesse einfließen.[67]

Durch diese Regelung wird der technische Datenschutz aus Sicht des Weizenbaum-Instituts pauschal und unnötig geschwächt.[68]

## 6.3 Vereinbarkeit mit Art. 16 ff. KI-VO

Die Europäische Kommission hat im sogenannten Digital-Omnibus[69] unter anderem einen Änderungsvorschlag für den Geltungsbeginn der Pflichten für Hochrisiko-KI-Systeme nach der KI-VO vorgeschlagen. Demnach sollen die Pflichten zu einem späteren Zeitpunkt gelten.[70] Die Rechtsgrundlagen für das Training von polizeilichen KI-Systemen sollten von den nationalen Gesetzgebern allerdings so ausgestaltet werden, dass sie nicht gegen zukünftig geltendes höherrangiges Recht verstoßen.

Die Polizei könnte *Anbieterin* i.S.d. KI-VO des KI-Systems sein. Dann müsste sie eine Reihe von Verpflichtungen erfüllen, deren Großteil in Art. 16 KI-VO gebündelt benannt ist. Anbieterin nach Art. 3 Nr. 3 KI-VO ist auch die Person oder Behörde, die ein KI-System entwickeln lässt und unter eigenem Namen in Betrieb nimmt. Ob eine Auftragsentwicklung vorliegt, dürfte davon abhängen, ob Einfluss auf den Entwicklungsprozess, etwa durch Bestimmen von Anforderungen, Spezifikationen oder Qualitätsstandards, ausgeübt wird.[71] Bei einem KI-System, dass die Polizei Berlin lediglich einkauft, dürfte eine Auftragsentwicklung regelmäßig noch nicht vorliegen. Je nach der tatsächlichen Beschaffung kann dieses Ergebnis jedoch variieren. Eine Inbetriebnahme kann schon im reinen Eigengebrauch einer eigenen

[67] Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI); Stellungnahme der Berliner Beauftragten für Datenschutz und Informationsfreiheit zum Änderungsantrag der Fraktion der CDU und der Fraktion der SPD zur Drucksache 19/2553: Gesetz zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, S.2.

[68] Vgl. Botta, Stellungnahme zum Gesetz zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin (AGH-Drs. 19/2553), S. 7.

[69] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus) COM/2025/837 final, 19.11.2025, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52025PC0837, zuletzt aufgerufen am 21.02.2025.

[70] Vgl. EU-Komm., Proposal for a Regulation of the European Parliament and of the Council, amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI), 19.11.2025, COM(2025) 836 final, 2025/0359 (COD), S. 30.

[71] Bomhard in: derselbe/Pieper/Wende, KI-VO, Art. 3 Rn. 97.

Anwendung liegen.[72] Soweit die Polizei Berlin ein KI-System entwickeln lässt und unter eigenem Namen verwendet, kann sie bereits als Anbieterin des KI-Systems nach der KI-VO gelten.

Sie könnte zudem als *Quasi-Anbieterin* nach Art. 25 Abs. 1 KI-VO in die Verantwortlichkeit der Anbieterin einrücken. Soweit ein KI-System mit einem staatlich festgelegten Namen verwendet wird, könnte die Behörde nach Art. 25 Abs. 1 li. a KI-VO als Quasi-Anbieterin gelten.[73] Die Weiterentwicklung eines entsprechenden KI-Systems kann eine wesentliche Änderung darstellen, wodurch die Behörde ebenfalls zur Quasi-Anbieterin wird.[74]

Das trainierte KI-System müsste ein Hochrisiko-KI-System nach Art. 6 Abs. 2 i.V.m. Anhang III KI-VO sein. Ein von der Polizei Berlin eingesetztes KI-System könnte insbesondere in den Bereich der Strafverfolgung nach Anhang III Nr. 6 fallen. Der Begriff der Strafverfolgung wird in Art. 3 Nr. 46 KI-VO definiert und umfasst die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder zur Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit. Der Begriff der Strafverfolgung in der KI-VO geht damit über den deutschen Begriff der Strafverfolgung hinaus[75] und umfasst auch die polizeiliche Gefahrenabwehr. Je nach konkreter Verwendung könnte schon das Training in den Anwendungsbereich des Anhang III KI-VO fallen. Wird das KI-System zur Bewertung des Risikos, dass eine natürliche Person eine Straftat begeht oder erneut begeht, verwendet, ist es ein Hochrisiko-KI-System nach Art. 6 Abs. 2 i.V.m. Anhang III Nr. 6 lit. d KI-VO.[76]

Zu den relevanten Pflichten im Zusammenhang mit dem Training und Testen eines KI-Systems dürfte insbesondere die Verpflichtung zur Daten-Governance nach Art. 10 i.V.m. 16 lit. a KI-VO zählen. Trainings-, Validierungs- und Testdatensätze müssen den in Art. 10 Abs. 2 bis 5 KI-VO festgelegten Qualitätskriterien entsprechen (Art. 10 Abs. 1 KI-VO). Weiterhin ist zu beachten, dass nach Art. 20 Abs. 1 S. 1 i.V.m. Art. 16 lit. j KI-VO Korrekturmaßnahmen ergriffen werden müssen, wenn die Behörde als Anbieterin Grund zur Annahme hat, dass das KI-System nicht den gesetzlichen Anforderungen der KI-VO entspricht. Die Pflicht soll sicherstellen, dass nach der Inbetriebnahme die Einhaltung der Anforderungen der KI-VO eingehalten werden.[77]

Bisher ist nicht geklärt, wie sich eine Verletzung der Art. 16 ff. KI-VO auf die Rechtmäßigkeit einer behördlichen Maßnahme auswirkt. Verstößt der Einsatz eines KI-Systems gegen die Art. 16 ff. KI-VO ist fraglich, ob Verwaltungsakte, die mithilfe des KI-Systems erlassen werden (etwa Datenanalyse als Entscheidungsgrundlage für Ermittlungsmaßnahmen), dann

[72] Bomhard in: derselbe/Pieper/Wende, KI-VO, Art. 3 Rn. 103.

[73] Vgl. Martini/Botta: Polizeiliche Datenanalyse mittels KI, DÖV 2025, S. 1033, 1038.

[74] Martini/Botta: Polizeiliche Datenanalyse mittels KI, DÖV 2025, S. 1033, 1038.

[75] Vgl. Klawonn in: BeckOK KI-Recht, 4. Ed. 1.11.2025, KI-VO Anhang III Rn. 88; Gehrmann in: Bomhard/Pieper/wende, KI-VO, Art. 6 Rn. 124.

[76] Vgl. Botta, Stellungnahme zum Gesetz zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin (AGH-Drs. 19/2553), S. 21.

[77] Vgl. Spittka, in: BeckOK KI-Recht, 4. Ed. 1.11.2025, KI-VO, Art. 20 Rn. 2.

rechtswidrig wären. Dies liegt darin begründet, dass das Verhältnis von europäischem Produktsicherheitsrecht und nationalem Gefahrenabwehrrecht weitestgehend noch nicht rechtswissenschaftlich untersucht worden ist.

## 6.4 Vereinbarkeit mit dem BlnDSG

Schließlich bleibt im Entwurf unklar, wie sich § 42d ASOG zu den allgemeinen Bestimmungen des BlnDSG verhält. Eine ausdrückliche Klarstellung, dass die Vorschrift nicht abschließend ist und insbesondere Betroffenenrechte, Informationspflichten und Aufsichtsmechanismen unberührt bleiben, wäre aus Sicht des Weizenbaum-Instituts erforderlich, um das unionsrechtlich garantierte Schutzniveau aufrechtzuerhalten.

Zusammenfassend lässt sich feststellen, dass aus Sicht des Weizenbaum-Instituts fraglich ist, ob der Erlaubnistatbestand des § 42d ASOG den unionsrechtlichen Anforderungen an Bestimmtheit, Verhältnismäßigkeit und rechtsstaatliche Absicherung genügt. Er eröffnet weitreichende Weiterverarbeitungsmöglichkeiten ohne ausreichende technische, organisatorische und verfahrensrechtliche Garantien und birgt damit erhebliche Risiken für den Schutz personenbezogener Daten im Kontext sicherheitsbehördlicher KI-Anwendungen. Zudem birgt er, wie weiter oben dargestellt, die Gefahr, dass zukünftig nach ihm erlassene Verwaltungsakte gegen die KI-VO verstoßen.

Die durch den Änderungsantrag aufgenommen Anpassungen führen aus Sicht des Weizenbaum-Instituts zu punktuellen Verbesserungen: Es wird ein ausdrückliches Verbot der Re-Identifizierung eingeführt, die unumkehrbare Anonymisierung ermöglicht und eine maximale Aufbewahrungsfrist von zwei Jahren festgelegt. Das Weizenbaum-Institut bewertet diese Maßnahmen als einen Schritt in Richtung technischer Datensicherheit, hält sie jedoch für unzureichend. Die zentralen Probleme bleiben bestehen: Die Zweckänderung ist weiterhin unzureichend geregelt, Diskriminierungsrisiken und Bias werden nicht ausreichend adressiert, die Einbindung privater Dritter bleibt unklar, sensible Daten können weiterhin verwendet werden, die Rechtmäßigkeit von auf den § 42d ASOG gestützten Maßnahmen vor dem Hintergrund der KI-VO und das Verhältnis zu allgemeinen Datenschutzbestimmungen bleiben ungeklärt.

- Das Weizenbaum-Institut empfiehlt, eine unabhängige wissenschaftliche und ethische Bewertung der Trainings- und Evaluierungsverfahren gesetzlich zu verankern, sowohl vor Inbetriebnahme als auch kontinuierlich während des Trainings. Dabei sollte die Betroffenenperspektive einbezogen werden, um Diskriminierungsrisiken dauerhaft zu überwachen und zu dokumentieren.

- Außerdem empfiehlt das Weizenbaum-Institut, Veröffentlichungspflichten hinsichtlich der eingesetzten Modelle zu verankern. Insbesondere die Bewertung, ob die Behörde *Anbieterin* im Sinne der KI-VO ist, die Wirkweise der Methode und die Ergebnisse unabhängiger Prüfungen sollten hierzu zählen, um Transparenz und öffentliche Kontrolle sicherzustellen.

- Weiterhin wird empfohlen, dass die personenbezogenen Daten nicht an Dritte weitergegeben werden und das Training stets nur unter Kontrolle der Polizei Berlin stattfindet.

# 7 Automatisierte Anwendung zur Analyse vorhandener Daten (§ 47a ASOG)

Die ASOG-Novelle führt mit § 47a ASOG eine neue Befugnisnorm für automatisierte Datenanalysen (Data-Mining) bei der Polizei Berlin ein. Die Norm erlaubt die umfassende Zusammenführung, Verknüpfung und Aufbereitung großer polizeilicher Datenbestände, darunter Vorgangs-, Fall-, Telekommunikations-, Register- und Internetdaten. Damit entsteht eine Multidatenbasis, die einen besonders intensiven Eingriff in das Grundrecht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG begründet.

## 7.1 Verfassungsmäßigkeit

Aus Sicht des Weizenbaum-Instituts fehlt in der ASOG-Novelle eine eigenständige, hinreichend qualifizierte Eingriffsschwelle, die die Datenzusammenführung selbst legitimieren könnte. Da die Norm nicht an eine, zumindest ihrer Art nach, konkretisierte Gefahr für besonders gewichtige Rechtsgüter anknüpft, kollidiert sie bereits in ihrer Struktur mit den Anforderungen an vorsorgende Datenspeicherungen und automatisierte Analysebefugnisse.

Zudem begrenzt die Novelle des ASOG weder die Art noch die Sensibilität oder Herkunft der verarbeitbaren Daten ausreichend. Es existiert kein ausdrücklicher Ausschluss besonders grundrechtssensibler Daten, auch nicht solcher, die aus schwerwiegenden Grundrechtseingriffen herrühren. Die Möglichkeit, ohne weitere Differenzierung nahezu alle polizeilich verfügbaren Daten zu integrieren, steigert das Eingriffsgewicht erheblich.

Ein weiterer Kritikpunkt betrifft die Offenheit der Analyseverfahren. Das ASOG erlaubt nach der Novellierung auch den Einsatz komplexerer, in bestimmten Fällen auch den Einsatz selbstlernender KI-Systeme. Automatisierte Entscheidungsfindungen und Sachverhaltsbewertungen sind nach § 47a Abs. 1 S. 6 ASOG unzulässig. Alle Ergebnisse der automatisierten Datenanalyse müssen aus den in § 47a Abs. 2 Satz 1 bis 4 ASOG genannten Daten durch menschliche Gedankengänge nachvollziehbar sein. Sollen in der Folge der automatisierten Datenanalyse Maßnahmen gegen Personen getroffen werden, dürfen diesen Maßnahmen allein Daten in einer nicht nach dem hiesigen Absatz verarbeiteten Fassung zugrunde gelegt werden. Positiv ist zunächst, dass die Norm nunmehr klarstellt, dass die Daten auf der Analyseplattform ausschließlich zur Vorbereitung der automatisierten Analyse zusammengeführt werden. Dies schränkt die Zweckbestimmung ein, ändert jedoch nichts daran, dass die Datenzusammenführung selbst weiterhin ohne qualifizierte Eingriffsschwelle erfolgt. Verbessert werden auch die Anlassvoraussetzungen: Für besonders eingriffsintensive Analysen

ist ein Bezug zu terroristischen Straftaten oder Katalogtaten der §§ 100a[78], 100b[79] StPO erforderlich. Diese Anpassung orientiert sich an der Rechtsprechung zu verdeckten Überwachungsmaßnahmen und hebt das Schutzniveau in bestimmten Konstellationen an; sollte jedoch aus Sicht des Weizenbaum-Instituts noch an die Rechtsprechung des Bundesverfassungsgerichts angepasst werden, welche die genannten strafprozessualen Normen teilweise für verfassungswidrig (und nichtig) erklärt hat.[80] Zudem verbleiben Kontexte, in denen niedrigere Anforderungen genügen, obwohl die betroffenen Datenmengen und Verarbeitungsmöglichkeiten gleichartig eingriffsintensiv sind. Eine wesentliche Korrektur bildet die nunmehr eindeutige Vorgabe, dass alle Analysen auf Suchbegriffen beruhen müssen, die aus einem konkreten Sachverhalt stammen. Dies reduziert das Risiko anlassloser algorithmischer Mustererkennung deutlich.

Auch der Einsatz selbstlernender Systeme wird auf Fälle besonders gewichtiger Rechtsgüter beschränkt und einer strengen Anordnungsbefugnis unterstellt. Die Stärkung der Nachvollziehbarkeit erfüllt ein Kernanliegen der verfassungsgerichtlichen Rechtsprechung. Begrüßenswert ist auch die Klarstellung, dass Folgemaßnahmen nicht auf maschinell vorverarbeitete Daten, sondern nur auf den Ausgangsdatenbestand gestützt werden dürfen. Dies verhindert, dass die Algorithmik selbst operative Tatsachengrundlagen schafft. Die ausdrückliche Pflicht zur Vermeidung algorithmischer Diskriminierung ist ein Schritt in die richtige Richtung. Ohne flankierende technische und organisatorische Kontrollinstrumente bleibt sie allerdings überwiegend deklaratorisch. Zudem stärken die aufgenommen Änderungen im Vergleich zum ursprünglichen Gesetzesentwurf Transparenz und Rechtsschutz, indem die Benachrichtigungspflicht nach § 42 BlnDSG für Maßnahmen, die auf Analyseergebnissen beruhen, nun gesetzlich klargestellt wird. Aus Sicht des Weizenbaum-Instituts erfüllen die gesetzlich verankerten Regelungen jedoch keine ausreichenden Absicherungen, um die Nutzung selbstlernender KI-Systeme zu gestatten.

Selbstlernende KI-Systeme sind in der polizeilichen Praxis kritisch zu bewerten, da sie unvorhersehbar, intransparent und rechtlich nicht ausreichend kontrollierbar sind, sodass ihr Einsatz die Einhaltung zentraler rechtsstaatlicher Anforderungen, speziell der Normenklarheit, der Nachvollziehbarkeit staatlichen Handelns und der effektiven Verantwortungszurechnung, gefährden kann, und dies auch im Kontext der Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung i.S.d. § 47a Abs. 1 S. 2 Nr. 1 und Nr. 3 ASOG.

---

[78] Das BVerfG hat am 24. Juni 2025 beschlossen: § 100a Absatz 1 Sätze 2 und 3 in Verbindung mit § 100a Absatz 1 Satz 1 Nummer 1, Absatz 2 Nummer 1 Buchstaben a, c, d und t, Nummer 6 und Nummer 7 Buchstabe b der Strafprozessordnung in der Fassung des Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 17. August 2017 (Bundesgesetzblatt I Seite 3202) und in der Fassung späterer Gesetze verstoßen nach Maßgabe der Gründe gegen Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 des Grundgesetzes sowie – nur bezogen auf § 100a Absatz 1 Satz 2 der Strafprozessordnung – auch gegen Artikel 10 Absatz 1 des Grundgesetzes und sind nichtig; vgl. 1 BvR 180/23.

[79] Das BVerfG hat am 24. Juni 2025 beschlossen: § 100b der Strafprozessordnung in der Fassung des Gesetzes zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 17. August 2017 und in der Fassung späterer Gesetze ist mit Artikel 10 Absatz 1 in Verbindung mit Artikel 19 Absatz 1 Satz 2 des Grundgesetzes unvereinbar. Die Vorschrift gilt bis zu einer Neuregelung fort; vgl. 1 BvR 180/23.

[80] Vgl. 1 BvR 180/23.

Trotz der vorgenommenen Verbesserungen bleibt der Kernkonflikt bestehen: Die Novelle des ASOG hält mit § 47a ASOG an einer dauerhaften, sehr weitreichenden Zusammenführung polizeilicher Datenbestände fest, ohne hierfür eine eigenständige, qualifizierte Eingriffsschwelle einzuführen, wie sie das Bundesverfassungsgericht für vergleichbare Datenplattformen verlangt. Die Norm bleibt in zentralen Punkten aus Sicht des Weizenbaum-Instituts unverhältnismäßig. Damit erfüllt § 47a ASOG in seiner Grundstruktur weiterhin nicht die verfassungsrechtlich erforderlichen Anforderungen an Normenklarheit, Verhältnismäßigkeit und grundrechtsschonende Ausgestaltung.

\\ Das Weizenbaum-Institut empfiehlt den Ausschluss selbstlernender KI-Systeme in der polizeilichen Praxis.

## 7.2 Unionsrechtmäßigkeit

### 7.2.1. Vereinbarkeit mit Art. 5 Abs. 1 lit. d KI-VO

Die KI-VO verbietet nicht pauschal den Einsatz von KI zur Strafverfolgung.[81] Das Verbot des Art. 5 Abs. 1 lit. d KI-VO umfasst den Einsatz eines KI-Systems, *„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.“*[82] Das Verhalten einer Person soll demnach nicht allein durch eine KI strafrechtlich beurteilt werden.[83] Eine Entscheidung durch KI ist folglich verboten, wenn ein Mensch zwar in die Entscheidung eingebunden wird, aber aufgrund seiner Qualifikation keine echte Überprüfungsinstanz darstellt oder die Empfehlung lediglich „mechanisch“ bestätigt.[84] Soweit eine menschliche Verdachtsbewertung lediglich mittels einer KI-gestützten Datenanalyse fundiert wird, ist dies noch nicht vom Verbot des Art. 5 Abs. 1 lit. d KI-VO erfasst.[85]

### 7.2.2. Vereinbarkeit mit Art. 86 KI-VO

Art. 86 Abs. 1 KI-VO statuiert ein sogenanntes „Recht auf Erläuterung der Entscheidungsfindung im Einzelfall“. Danach sind Betreiber:innen von Hochrisiko-KI-Systemen dazu verpflichtet, eine Entscheidung, die auf Grundlage der Ausgabe eines Hochrisiko-KI-Systems (nach Anhang III KI-VO), getroffen wurde, der betroffenen Person zu erläutern. Diese Pflicht greift jedoch nur, wenn die Entscheidung rechtliche Auswirkungen hat oder die Person in ähnlicher Art erheblich auf eine Weise beeinträchtigt, die ihrer Ansicht nach ihre Gesundheit, ihre Sicherheit oder ihre Grundrechte beeinträchtigt. Eine Beeinträchtigung eines Grundrechts könnte in der Weiterverarbeitung personenbezogener Daten liegen und die betroffene Person in ihrem Grundrecht auf Datenschutz nach Art. 7, 8 GRC verletzen. Selbst

[81] Martini/Botta: Polizeiliche Datenanalyse mittels KI, DÖV 2025, S. 1033, 1037.

[82] Vgl. Art. 5 Abs. 1 lit. d KI-VO.

[83] Raue, in: BeckOK KI-Recht, 4. Ed. 1.11.2025, KI-VO, Art. 5 Rn. 66.

[84] Wendehorst, in: Martini/dieselbe, KI-VO, Art. 5 Rn. 84.

[85] Martini/Botta: Polizeiliche Datenanalyse mittels KI, DÖV 2025, S. 1033, 1037.

wenn man dies ablehnt, so würde eine polizeiliche Maßnahme, die mithilfe des trainierten KI-Systems durchgeführt wird, der betroffenen Person gegenüber rechtliche Auswirkungen haben oder sie in ihren Grundrechten beeinträchtigen.

Fraglich ist darüber hinaus, wer *Betreiber:in* des KI-Systems wäre. *Betreiber:in* ist eine „natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System in eigener Verantwortung verwendet, es sei denn, das KI-System wird im Rahmen einer persönlichen und nicht beruflichen Tätigkeit verwendet“ (Art. 3 Nr. 4 KI-VO). Betreiberin kann demnach auch eine Behörde selbst sein. In eigener Verwendung schließt weisungsgebunden handelnde Personen regelmäßig vom Betreiberbegriff aus.[86] Daher wäre die Polizeibehörde selbst und nicht die einzelnen Beamt:innen Betreiberin oder Anbieterin.

Die Rechtsfolge des Art. 86 Abs. 1 KI-VO ist, dass der oder die Betreiber:in klar und aussagekräftig die Rolle des KI-Systems im Entscheidungsprozess und die wichtigsten Elemente der getroffenen Entscheidung erläutern muss. Dies bedeutet, dass auch KI-gestützte polizeiliche Maßnahmen (gleich ob präventiv oder repressiv) für Betroffene erklärbar sein müssen. In diesem Kontext ist positiv hervorzuheben, dass § 47a Abs. 1 S. 6 ASOG statuiert, dass alle Ergebnisse der automatisierten Datenanalyse durch menschliche Gedankengänge nachvollziehbar sein müssen.

Darüber hinaus sollte aus Sicht des Weizenbaum-Instituts betroffenen Personen auf Verlangen dargelegt werden können, welche Rolle der KI-Einsatz im Rahmen der behördlichen Entscheidung gespielt hat. Weiterhin sollten die wesentlichen Entscheidungselemente nachvollziehbar dargelegt werden.

### 7.2.3. Vereinbarkeit mit Art. 26 Abs. 2 KI-VO

Soweit es sich bei dem KI-System um ein Hochrisiko-KI-System handelt, muss die menschliche Aufsicht über das System einer Person übertragen werden, die über die erforderliche Kompetenz, Ausbildung und Befugnis verfügt. Demnach muss für die Überwachung des KI-System eine Person eingesetzt werden, die über ausreichend KI-Kompetenz verfügt. Es ist zu begrüßen, dass nach § 47a Abs. 3 S. 1 ASOG nur ausgewählte und geschulte Polizeidienstkräfte Zugriff auf die automatisierte Datenanalyse haben dürfen. Ebenfalls positiv hervorzuheben ist, dass nach § 47a Abs. 3 S. 2 ASOG beim Einsatz selbstlernender Systeme die automatisierte Datenanalyse nur durch die Leitung des Landeskriminalamtes, deren Vertretung im Amt oder durch von dieser besonders beauftragte Beamtinnen oder Beamte des höheren Dienstes angeordnet werden darf.

[86] Vgl. Wendehorst in: Martini/dieselbe, KI-VO, Art. 3 Rn. 84.

# 8 Zusammenfassung

Die ASOG-Novelle enthält eine Vielzahl von Regelungen, die in erheblichem Umfang in grundrechtlich geschützte Bereiche eingreifen. Zwar ist die Anpassung sicherheitsrechtlicher Befugnisse an digitale Herausforderungen grundsätzlich durch den Schutzauftrag des Staates geboten, dennoch ist der Einsatz digitaler Techniken und Technologien nicht zwingend erforderlich. Die analysierten Vorschriften zeigen, dass zentrale Anforderungen an Verhältnismäßigkeit, Normenklarheit und Transparenz nicht hinreichend berücksichtigt sind. Dies betrifft insbesondere die Ausweitung der Videoüberwachung, den Einsatz von Body-Cams, Einführung automatisierter Verhaltensanalysen sowie die Nutzung polizeilicher Daten für KI-Systeme und den Abgleich von biometrischen Daten mit im Internet allgemein verfügbaren Daten. In ihrer derzeitigen Form bleiben diese Regelungen hinter den verfassungsrechtlichen und unionsrechtlichen Anforderungen aus Sicht des Weizenbaum-Instituts zurück.

# Impressum

**Weizenbaum-Institut**
Stellungnahme zur Novellierung des Allgemeinen Sicherheits- und Ordnungsgesetzes Berlin (ASOG Bln). Drucksache 19/2553 und Änderungsantrag der Fraktion der CDU und der Fraktion der SPD zur Drucksache 19/2553

Weizenbaum Policy Paper # 19
Berlin, März 2026

ISSN 2940-8490 \ DOI 10.34669/WI.PP/19

**Weizenbaum-Institut e.V.**
Hardenbergstraße 32 \ 10623 Berlin \ Tel.: +49 30 700141-001
info@weizenbaum-institut.de \ www.weizenbaum-institut.de



**KOORDINATION:** Dr. Moritz Buchner



weizenbaum institut

Gefördert durch:
Bundesministerium für Forschung, Technologie und Raumfahrt
BERLIN Senatsverwaltung für Wissenschaft, Gesundheit und Pflege