

Schleswig-Holsteinischer Landtag
Umdruck 20/7129

Stellungnahme

zum

**Gesetzesentwurf zur Fortentwicklung polizeirechtlicher Maßnahmen für einen wirk-
samen Schutz der öffentlichen Sicherheit und zum Änderungsantrag der Fraktionen
von CDU und BÜNDNIS 90/DIE GRÜNEN**

(LT-Drs. 20/4284 und LT-Umdruck 20/6786)

zu Händen von Herrn Jan Kürschner, Vorsitzender des Innen- und Rechtsausschusses

09.09.2026

BROCK MÜLLER ZIEGENBEIN
Rechtsanwälte Partnerschaft mbB Notare
RA Dr. Simon Diethelm Meyer
Schwedenkai 1, 24103 Kiel

E-Mail: simon.meyer@bmz-recht.de
www.bmz-recht.de

Sehr geehrter Herr Vorsitzender Kürschner,

sehr geehrte Damen und Herren,

mit E-Mail vom 25.06.2026 haben Sie mir freundlicherweise die Gelegenheit eingeräumt, zu dem in der o.a. Drucksache vorgeschlagenen Gesetzesentwurf Stellung zu nehmen. Dafür bedanke ich mich herzlich und komme dem Anliegen gern nach.

Inhaltsübersicht

I. Allgemeine Erwägungen	2
II. IT-gestützter Abgleich und Datenanalyse, §§ 188c, 188d LVwGE.....	3
1. Eingriffsschwellen	3
2. Verfahrensrechtliche Vorkehrungen	6
3. Digitale Souveränität	7
III. Echtzeit-Fernidentifizierung in öffentlich zugänglichen Räumen, §§ 184b, 184c LVwGE	8
1. Vorgaben der KI-Verordnung.....	9
2. Verfassungsrechtliche Anforderungen	10
IV. Nachträgliche Fernidentifizierung, §§ 195b, 195c LVwGE	12
1. Vorgaben der KI-Verordnung.....	12
2. Verfassungsrechtliche Anforderungen	13
V. Gewahrsam von Personen, §§ 204, 205, 205a LVwGE	14
1. Zur Höchstdauer des Gewahrsams, § 204 Abs. 6 Satz 2 LVwGE.....	15
2. Zum Gewahrsam für Begleitpersonen, § 204 Abs. 1 Nr. 2 Halbsatz 2 Buchst. b LVwGE.....	17
VI. Maßnahmen gegen unbemannte Fahrzeugsysteme, § 213a LVwGE	18
VII. Zusammenfassung.....	20

I. Allgemeine Erwägungen

Der Gesetzesentwurf verfolgt das Ziel, das Polizeirecht des Landes Schleswig-Holstein an aktuelle Herausforderungen anzupassen. Hierfür weitert der Gesetzesentwurf die polizeilichen Befugnisse, insbesondere im digitalen Bereich, erheblich aus. Der Änderungsantrag der

Fraktionen von CDU und BÜNDNIS 90/DIE GRÜNEN ergänzt den Gesetzesentwurf um weitere Standardermächtigungen, etwa im Zusammenhang mit unbemannten Fahrzeugsystemen.

Jede rechtsstaatliche Sicherheitsgesetzgebung steht vor einem unauflöslichen Dilemma:¹ Um die Freiheit der Menschen zu schützen, muss der Staat in Freiheitsrechte eingreifen. Der Staat ist zu Freiheitseingriffen nicht nur berechtigt, sondern aufgrund grundrechtlicher Schutzpflichten, etwa aus Art. 2 Abs. 2 Satz 1 GG, sogar verpflichtet. Allerdings dürfen die staatlichen Freiheitseingriffe nicht über das erforderliche und angemessene Maß hinausgehen. Ein Rechtsstaat darf, weil er Rechtsstaat ist, von Eingriffsinstrumenten nicht in ähnlich schrankenloser Weise Gebrauch machen wie kriminelle Akteure. Die Herausforderung für den Landesgesetzgeber besteht darin, eine ausgewogene Balance zwischen Freiheit und Sicherheit zu finden.

Im Folgenden werden die einzelnen Regelungen des Gesetzesentwurfs rechtlich eingeordnet. Dabei beschränkt sich die Stellungnahme auf diejenigen Bestimmungen, die nach Ansicht des Verfassers besondere rechtliche Fragen aufwerfen. Soweit erforderlich oder zweckmäßig, werden Änderungen vorgeschlagen.

II. IT-gestützter Abgleich und Datenanalyse, §§ 188c, 188d LVwGE

Die Regelungen zum IT-gestützten Abgleich und zur Datenanalyse (§§ 188c, 188d LVwGE) werfen Fragen im Hinblick auf Eingriffsschwellen, verfahrensrechtliche Vorkehrungen sowie digitale Souveränität auf.²

1. Eingriffsschwellen

Die verfassungsrechtlichen Eingriffsschwellen ergeben sich maßgeblich aus dem Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 2 GG). Diesen Anforderungen im Kontext der automatisierten Datenanalyse hat das Bundesverfassungsgericht in seinem grundlegenden Urteil vom 16.02.2023³ konkretisiert. Demnach ergeben sich das Eingriffsgewicht einer automatisierten Datenanalyse oder –auswertung und die verfassungsrechtlichen Rechtfertigungsanforderungen zum einen aus dem

¹ Vgl. *Meyer*, GSZ 2025, 156 (156), auch zum Folgenden.

² Siehe hierzu und zum Folgenden *Meyer*, GSZ 2025, 156 (156 ff.).

³ BVerfG, Urteil vom 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196.

Gewicht der vorausgegangenen Datenerhebungseingriffe; insoweit gelten die Grundsätze der Zweckbindung und Zweckänderung.⁴ Zum anderen hat die automatisierte Datenanalyse oder -auswertung potenziell ein Eigengewicht, sodass weitergehende Rechtfertigungsanforderungen gelten.⁵

Ermöglicht die automatisierte Anwendung einen schwerwiegenden Eingriff in die informationelle Selbstbestimmung der Betroffenen, ist sie nur unter den engen Voraussetzungen für eingriffsintensive heimliche Überwachungsmaßnahmen zu rechtfertigen. Sowohl die zu schützenden Rechtsgüter als auch der Eingriffsanlass müssen eng begrenzt sein: Heimliche Überwachungsmaßnahmen sind nur zum Schutz besonders gewichtiger Rechtsgüter zulässig, insbesondere zum Schutz von Leib, Leben und Freiheit der Person, Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, sowie Bestand oder Sicherheit des Bundes oder eines Landes.⁶ Als Eingriffsanlass bedarf es einer hinreichend konkretisierten Gefahr; es müssen also zumindest tatsächliche Anhaltspunkte für die Entstehung einer konkreten Gefahr für die Schutzgüter bestehen.⁷

Weniger gewichtige Eingriffe lassen sich beim Vorliegen einer konkretisierten Gefahr bereits dann rechtfertigen, wenn sie dem Schutz von Rechtsgütern von zumindest erheblichem Gewicht dienen, wie dies etwa bei der Verhütung von Straftaten von zumindest erheblicher Bedeutung der Fall ist. Umgekehrt kann dann eine Eingriffsschwelle genügen, die noch hinter einer konkretisierten Gefahr zurückbleibt, wenn die Maßnahme dem Schutz hochrangiger, überragend wichtiger oder auch besonders gewichtiger Rechtsgüter dient. Jeweils ist allerdings erforderlich, dass der Gesetzgeber das Eingriffsgewicht der Datenanalyse oder -auswertung durch eine strengere Regelung zu Art und Umfang der verwertbaren Daten und zur Verarbeitungsmethode verringert.⁸ Auf die Schwelle einer wenigstens konkretisierten Gefahr für besonders gewichtige Rechtsgüter kann der Gesetzgeber nur dann verzichten, wenn die zugelassenen Analyse- und Auswertungsmöglichkeiten normenklar und hinreichend bestimmt in der Sache so eng begrenzt sind, dass das Eingriffsgewicht der Maßnahmen erheblich gesenkt ist.⁹

⁴ BVerfG, Urteil vom 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 Rn. 54.

⁵ BVerfG, Urteil vom 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 Rn. 54.

⁶ BVerfG, Urteil vom 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 Rn. 103 ff.

⁷ BVerfG, Urteil vom 20.04.2016 – 1 BvR 966/09, 1 BvR 1140/09, NJW 2016, 1781 Rn. 112; BVerfG, Urteil vom 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 Rn. 106.

⁸ BVerfG, Urteil vom 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 Rn. 107.

⁹ BVerfG, Urteil vom 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 Rn. 110.

Will der Gesetzgeber die Eingriffsintensität der automatisierten Datenanalyse oder –auswertung reduzieren, um sie auch im Vorfeld einer konkretisierten Gefahr einsetzen zu können, muss er grundlegende Vorgaben zu Art und Umfang der in der automatisierten Datenanalyse oder –auswertung verwendbaren Daten selbst regeln. Erforderlich ist insbesondere eine gesetzliche Regelung, welche Datenbestände einbezogen werden dürfen und inwiefern dies automatisiert erfolgen darf.¹⁰ Zudem muss der Gesetzgeber einschränkende Vorgaben zur Methode der automatisierten Datenanalyse machen und in ihren grundlegenden Zügen im Gesetz selbst regeln. Der Einsatz selbstlernender Systeme muss hierfür im Gesetz ausdrücklich ausgeschlossen sein.¹¹

Diesen verfassungsrechtlichen Anforderungen wird der Gesetzesentwurf grundsätzlich gerecht.¹² Der Gesetzesentwurf unterscheidet zwischen dem IT-gestützten Abgleich (§ 188c Abs. 1 LVwGE), der lediglich ein geringes Eingriffsgewicht aufweist, der automatisierten Datenanalyse mit reduziertem Eingriffsgewicht (§ 188c Abs. 3 LVwGE) sowie der automatisierten Datenanalyse mit hohem Eingriffsgewicht (§ 188c Abs. 4 LVwGE). Entsprechend dem Eingriffsgewicht werden die Maßnahmen an gestufte Eingriffsschwellen geknüpft. Die Eingriffsschwellen entsprechen den verfassungsrechtlichen Anforderungen nicht nur, sondern gehen teilweise sogar über diese hinaus.¹³

Zweifelhaft ist indes, ob die Ermächtigung zur Erstellung eines Verhaltensprofils bei einer Datenanalyse mit reduziertem Eingriffsgewicht (§ 188c Abs. 7 Satz 1, Satz 2 LVwGE) mit dem Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) vereinbar ist.¹⁴ Nach Ansicht des Bundesverfassungsgerichts ist jede „Erstellung von genaueren Bewegungs-, Verhaltens- oder Beziehungsprofilen“ ein schwerer Eingriff in die informationelle Selbstbestimmung, der sich nur unter den engen Voraussetzungen für eingriffsintensive heimliche Überwachungsmaßnahmen rechtfertigen lässt.¹⁵ Diese engen Voraussetzungen sind bei der Datenanalyse mit reduziertem Eingriffsgewicht (§ 188c Abs. 3 LVwGE) nicht erfüllt. § 188c Abs. 7 Satz 2 LVwGE sieht vor, dass das Verhaltensprofil im Falle einer Datenanalyse nach Absatz 3 höchstens den Zeitraum von einer Woche umfassen darf. Bereits anhand der Verkehrsdaten für eine Woche kann indes ein umfassendes Verhaltensprofil einer Person erstellt werden.¹⁶ Die zeitliche Beschränkung

¹⁰ BVerfG, Urteil vom 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 Rn. 115 f.

¹¹ BVerfG, Urteil vom 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 Rn. 120 f.

¹² Vgl. *Heckmann/Klauser/Ziegler*, LT-Umdruck 20/6959, S. 11 f.

¹³ Vgl. LT-Drs. 20/4284, S. 52.

¹⁴ Vgl. *Heckmann/Klauser/Ziegler*, LT-Umdruck 20/6959, S. 12.

¹⁵ BVerfG, Urteil vom 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 Rn. 73.

¹⁶ *Heckmann/Klauser/Ziegler*, LT-Umdruck 20/6959, S. 9 f. m.w.N.

in § 188c Abs. 7 Satz 2 LVwGE ist daher nicht geeignet, das Eingriffsgewicht der Profilbildung wesentlich zu reduzieren.

Um verfassungsrechtliche Risiken zu vermeiden, sollte die Ermächtigung zur Erstellung eines Verhaltensprofils in § 188c Abs. 7 LVwGE auf die Datenanalyse mit hohem Eingriffsgewicht (§ 188c Abs. 4 LVwGE) beschränkt werden. Die Erstellung eines Verhaltensprofils wäre demnach nur zur Abwehr einer Gefahr nach § 188c Abs. 4 LVwGE zulässig. Eine entsprechende Regelung könnte wie folgt lauten:

„Durch eine Datenanalyse darf ein Profil über das Verhalten einer Person nur dann erstellt werden, wenn Tatsachen die Annahme rechtfertigen, dass diese Person für die Gefahr verantwortlich ist und das Verhaltensprofil zur Abwehr der Gefahr nach Absatz 4 erforderlich ist.“

2. Verfahrensrechtliche Vorkehrungen

Nach der Rechtsprechung des Bundesverfassungsgerichts dürfen selbstlernende Systeme in der Polizeiarbeit nur unter besonderen verfahrensrechtlichen Vorkehrungen zur Anwendung kommen, die trotz der eingeschränkten Nachvollziehbarkeit ein hinreichendes Schutzniveau sichern.¹⁷ Zudem stellt der Verhältnismäßigkeitsgrundsatz Anforderungen an Transparenz, individuellen Rechtsschutz und aufsichtliche Kontrolle.¹⁸ Für eine effektive Kontrolle unerlässlich ist dabei, dass eigenständig ausformulierte Begründungen dafür gegeben werden, warum bestimmte Datenbestände zur Verhütung bestimmter Straftaten im Wege automatisierter Anwendung analysiert werden. Wird Software eingesetzt, die komplexere Formen des automatisierten Abgleichs von Daten erlaubt, sind auch Vorkehrungen gegen eine hiermit spezifisch verbundene Fehleranfälligkeit erforderlich, was auch gesetzliche Regelungen zu einem staatlichen Monitoring der Entwicklung der eingesetzten Software erfordern kann.¹⁹ In Betracht kommen interne Evaluations- und Qualitätssicherungsmaßnahmen im Hinblick auf die Methodik und Ergebnisse der Verfahren.²⁰ Das eingesetzte KI-System muss in einem wissenschaftlich anerkannten Verfahren entwickelt worden sein und dem aktuellen Stand der Technik entsprechen. Sein Einsatz muss fortlaufend durch sachkundiges Personal überwacht werden, um potentielle

¹⁷ BVerfG, Urteil vom 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 Rn. 100.

¹⁸ BVerfG, Urteil vom 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 Rn. 109.

¹⁹ BVerfG, Urteil vom 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 Rn. 109.

²⁰ Kugelmann/Buchmann, GSZ 2024, 1 (9); Meyer, GSZ 2025, 156 (159).

Fehlerquellen so früh wie möglich zu erkennen. Darüber hinaus ist eine ausreichende Datenqualität sicherzustellen.²¹ Die verwendeten Datenbestände dürfen ausschließlich richtige, aktuelle und rechtmäßig gespeicherte Daten enthalten.²²

Eine besondere Herausforderung ergibt sich aus dem Einsatz diskriminierender Algorithmen. Beim Prozess maschinellen Lernens können KI-Systeme Stereotype („Bias“) ausbilden, die zu diskriminierenden Entscheidungen zum Nachteil bestimmter Bevölkerungsgruppen führen.²³ Der Gesetzgeber muss daher Vorkehrungen treffen, um die Herausbildung und Verwendung diskriminierender Algorithmen zu verhindern.²⁴

Entsprechende verfahrensrechtliche Vorkehrungen enthält der Gesetzesentwurf bislang nicht. Daher ist zweifelhaft, ob die Bestimmungen zur automatisierten Datenanalyse (§§ 188c, 188d LVwGE) mit dem Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) und dem Rechtsstaatsprinzip (Art. 20 Abs. 3 GG) vereinbar sind. Um verfassungsrechtliche Risiken zu vermeiden, sollten die §§ 188c, 188d LVwGE um verfahrensrechtliche Vorkehrungen ergänzt werden. Diese sollten insbesondere Regelungen zur Gewährleistung einer hinreichenden Datenqualität sowie zur regelmäßigen Überprüfung der verwendeten Systeme umfassen.

3. Digitale Souveränität

Der Grundsatz digitaler Souveränität folgt aus dem Rechtsstaatsprinzip (Art. 20 Abs. 3 GG) und dem Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG).²⁵ Das Rechtsstaatsprinzip verpflichtet den Staat, Eingriffe in Grundrechte nachvollziehbar zu begründen.²⁶ Zudem hat der Staat ein Eigeninteresse an der Hoheit über die von ihm verwendeten IT-Systeme, um Abhängigkeiten zu vermeiden. Wird eine von privaten Dritten oder ausländischen Staaten entwickelte Software

²¹ BVerfG, Urteil vom 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 Rn. 95.

²² Buchmann/Kugelman, Verfassungsblog vom 11.12.2024; Meyer, GSZ 2025, 156 (159).

²³ Vgl. Lauscher/Legner, ZfDR 2022, 367 (369 ff.); Wischmeyer, AöR 143 (2018), 1 (26 ff.); Meyer, GSZ 2025, 156 (159).

²⁴ Vgl. BVerfG, Urteil vom 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 Rn. 100.

²⁵ Vgl. Roßnagel, MMR 2023, 64 (66 f.); Kelber/Bortnikov, NJW 2023, 2000 (2001 f.); Bäuerle, ZD 2025, 128 (131); Meyer, GSZ 2025, 156 (160); dens., LTO vom 14.08.2025.

²⁶ Vgl. Ibold, GSZ 2024, 10 (12).

eingesetzt, besteht überdies die Gefahr unbemerkter Manipulation oder des unbemerkten Zugriffs auf Daten durch Dritte.²⁷

Aus verfassungsrechtlicher Sicht ist das Outsourcing von IT-Anwendungen eine rechtfertigungsbedürftige Ausnahme: Je grundrechtsrelevanter ein System ist, desto schwerer lässt sich ein IT-Outsourcing rechtfertigen. Für grundrechtsrelevante KI-Systeme gilt daher der Grundsatz des Vorrangs der Eigenentwicklung.²⁸ Um eine rechtsstaatlich nicht hinnehmbare Abhängigkeit der Sicherheitsbehörden von Dritten zu vermeiden, sind Eigenentwicklungen sowie Open-Source-Komponenten zu bevorzugen.²⁹ Nur dann, wenn eine Eigenentwicklung nicht möglich oder nicht gleichermaßen effektiv wäre, dürfen die Sicherheitsbehörden auf KI-Systeme privater Anbieter oder ausländischer Staaten zurückgreifen.³⁰ Dabei genießen KI-Systeme aus der Europäischen Union den Vorrang gegenüber KI-Systemen aus Drittstaaten, die nicht über ein vergleichbares Datenschutzniveau verfügen.

In §§ 188c, 188d LVwGE fehlen Regelungen zur Sicherung digitaler Souveränität. Nach dem Gesetzeswortlaut wäre also etwa auch der Einsatz von Software des US-amerikanischen Unternehmens Palantir Technologies Inc. zulässig. Die Auswahl der Software bleibt letztlich der Exekutive überlassen. Vor diesem Hintergrund empfiehlt es sich, den Gesetzesentwurf um ausdrückliche Regelungen zur Sicherung digitaler Souveränität zu ergänzen. Insbesondere sollte ein Vorrang von Eigenentwicklungen und Open-Source-Komponenten sowie Software aus der Europäischen Union gesetzlich festgeschrieben werden.

III. Echtzeit-Fernidentifizierung in öffentlich zugänglichen Räumen, §§ 184b, 184c LVwGE

§§ 184b, 184c LVwGE ermächtigen die Polizei zur biometrischen Echtzeit-Fernidentifizierung in öffentlich zugänglichen Räumen. Die biometrische Fernidentifizierung gehört zu den eingriffsintensivsten Maßnahmen der Polizei im digitalen Bereich.³¹ Sie ermöglicht es der Polizei, eine Person anhand biometrischer Merkmale, z.B. des Gesichts, zu identifizieren. Hierfür kombiniert die biometrischen Echtzeit-Fernidentifizierung die polizeilichen Maßnahmen der Videoüberwachung und der automatisierten Datenanalyse derart, dass eine neue

²⁷ BVerfG, Urteil vom 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 Rn. 100.

²⁸ Kelber/Bortnikov, NJW 2023, 2000 (2002); Bäuerle, ZD 2025, 128 (131); Meyer, GSZ 2025, 156 (160).

²⁹ Kelber/Bortnikov, NJW 2023, 2000 (2002); Meyer, GSZ 2025, 156 (160).

³⁰ Meyer, GSZ 2025, 156 (160).

³¹ Coombe/Roth-Isigkeit, ZfDR 2024, 391 (415).

Eingriffsintensität entsteht.³² In Politik und Wissenschaft ist die Zulässigkeit der biometrischen Fernidentifizierung umstritten.³³ Die Regelungen der §§ 184b, 184c LVwGE unterliegen sowohl unionsrechtlichen als auch verfassungsrechtlichen Anforderungen.

1. Vorgaben der KI-Verordnung

Nach Art. 5 Abs. 1 Satz 1 Buchst. h KI-VO ist die Verwendung biometrischer Echtzeit-Fernidentifikationssysteme zu Strafverfolgungszwecken in öffentlich zugänglichen Räumen grundsätzlich verboten und nur ausnahmsweise unter strengen Voraussetzungen zulässig.³⁴ Der Begriff der „Strafverfolgung“ im Sinne der KI-Verordnung umfasst nach Art. 3 Nr. 46 KI-VO auch die Gefahrenabwehr. Die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme muss gemäß Art. 5 Abs. 1 Satz 1 Buchst. h KI-VO unbedingt erforderlich sein, um gezielt nach bestimmten Opfern von Entführung, Menschenhandel oder sexueller Ausbeutung sowie nach vermissten Personen zu suchen (Buchst. i), eine konkrete, erhebliche und unmittelbare Gefahr für das Leben oder die körperliche Unversehrtheit natürlicher Personen oder eine tatsächliche und bestehende oder tatsächliche und vorhersehbare Gefahr eines Terroranschlags abzuwenden (Buchst. ii) oder eine Person aufzuspüren oder zu identifizieren, die der Begehung einer schweren Straftat verdächtig ist (Buchst. iii). Nach Art. 5 Abs. 2 KI-VO darf die Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme nur zur Bestätigung der Identität der speziell betroffenen Person erfolgen, wobei die Art der Situation (Buchst. a) sowie die Folgen der Verwendung des Systems für die Rechte und Freiheiten aller betroffenen Personen (Buchst. b) zu berücksichtigen sind. Art. 5 Abs. 3 KI-VO enthält einen relativen Richtervorbehalt. Diesen Anforderungen werden die §§ 184b, 184c LVwGE durch hohe Eingriffsschwellen und den Richtervorbehalt des § 184b Abs. 3 LVwGE gerecht.

Darüber hinaus gelten für die biometrischer Echtzeit-Fernidentifikationssysteme die Anforderungen an Hochrisiko-KI-Systeme. Hochrisiko-KI-Systeme unterliegen nach Art. 8 Abs. 1, 9 ff. KI-VO umfassenden Dokumentations-, Informations- und Aufklärungspflichten.³⁵ Die Art. 9 ff. KI-VO enthalten Vorgaben zum Risikomanagement (Art. 9 KI-VO), zu Daten und Daten-Governance (Art. 10 KI-VO), zur technischen Dokumentation (Art. 11 KI-VO), zu Aufzeichnungspflichten (Art. 12 KI-VO), zur Transparenz und

³² *Coombe/Roth-Isigkeit*, ZfDR 2024, 391 (394).

³³ Vgl. *Heckmann/Klauser/Ziegler*, LT-Umdruck 20/6959, S. 13 m.w.N.

³⁴ S. hierzu und zum Folgenden *Meyer*, GSZ 2025, 156 (159 f.).

³⁵ Siehe hierzu und zum Folgenden *Meyer*, GSZ 2025, 156 (160).

Bereitstellung von Informationen für die Betreiber (Art. 13 KI-VO), zur menschlichen Aufsicht (Art. 14 KI-VO) sowie zur Genauigkeit, Robustheit und Cybersicherheit (Art. 15 KIVO). In Art. 26 f. KI-VO sind Pflichten der Betreiber von Hochrisiko-KI-Systemen normiert. Nach Art. 26 Abs. 1 KI-VO müssen die Betreiber von Hochrisiko-KI-Systemen durch geeignete technische und organisatorische Maßnahmen sicherstellen, dass sie solche Systeme entsprechend den den Systemen beigefügten Betriebsanleitungen und im Einklang mit Art. 26 Abs. 3 und Abs. 6 KI-VO verwenden. Gemäß Art. 26 Abs. 2 KI-VO übertragen die Betreiber natürlichen Personen, die über die erforderliche Kompetenz, Ausbildung und Befugnis verfügen, die menschliche Aufsicht und lassen ihnen die erforderliche Unterstützung zukommen. Soweit die Eingabedaten ihrer Kontrolle unterliegen, sorgen die Betreiber nach Art. 26 Abs. 4 KI-VO dafür, dass die Eingabedaten der Zweckbestimmung des Hochrisiko-KI-Systems entsprechen und ausreichend repräsentativ sind. Vor der Inbetriebnahme eines Hochrisiko-KI-Systems haben öffentliche Stellen nach Art. 27 Abs. 1 KI-VO eine Grundrechte-Folgeabschätzung durchzuführen. Diese Anforderungen müssen bei der praktischen Anwendung der §§ 184b, 184c LVwGE beachtet werden.

2. Verfassungsrechtliche Anforderungen

Neben den unionsrechtlichen Vorgaben unterliegt die biometrische Fernidentifizierung auch verfassungsrechtlichen Anforderungen. Diese ergeben sich insbesondere aus dem Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG). Bislang hat das Bundesverfassungsgericht nicht über die Zulässigkeit der biometrischen Echtzeit-Fernidentifizierung entschieden. Daher ist auf die allgemeinen sicherheitsrechtlichen Grundsätze zurückzugreifen.³⁶

Als Kombination von Videoüberwachung und automatisierter Datenanalyse muss die biometrische Fernidentifizierung zumindest den Anforderungen genügen, die für diese beiden polizeilichen Maßnahmen gelten. Darüber hinaus ist das besondere Eingriffsge-
wicht der biometrischen Fernidentifizierung zu berücksichtigen. Die biometrische Fernidentifizierung hat eine erhebliche Streubreite, da sie auch zahlreiche unbeteiligte Personen betrifft.³⁷ Zudem betrifft die biometrische Fernidentifizierung biometrische Merkmale wie etwa körperliche Eigenschaften des Gesichts, die unveränderlich und daher

³⁶ Vgl. *Heckmann/Klauser/Ziegler*, LT-Umdruck 20/6959, S. 14.

³⁷ *Heckmann/Klauser/Ziegler*, LT-Umdruck 20/6959, S. 15.

besonders sensibel sind.³⁸ Auch Missbrauchs- und Diskriminierungsgefahren sowie mögliche Einschüchterungseffekte erhöhen das Eingriffsgewicht.³⁹ Dies gilt insbesondere, aber nicht ausschließlich beim Einsatz selbstlernender Systeme. Insgesamt hat die biometrische Fernidentifizierung ein sehr hohes Eingriffsgewicht. Deshalb unterliegt sie besonders strengen verfassungsrechtlichen Rechtfertigungsanforderungen. Die Begründung des Gesetzesentwurfs verweist darauf, dass die Grundsätze des Bundesverfassungsgerichts zur Rasterfahndung Anwendung finden.⁴⁰ Diesen Anforderungen werden die §§ 184b, 184c LVwGE gerecht.

Zweifelhaft ist allerdings, ob der Gesetzesentwurf auch dem besonderen Eingriffsgewicht der biometrischen Fernidentifizierung Rechnung trägt. Das Bundesverfassungsgericht hat in seiner Entscheidung zur automatisierten Datenanalyse ausgeführt, dass der Einsatz von KI-Systemen das Eingriffsgewicht einer Maßnahme erhöhen kann.⁴¹ Daher ist eine Übertragung der Grundsätze zur Rasterfahndung nicht zwingend. Insgesamt bestehen Zweifel, ob die §§ 184b, 184c LVwGE den verfassungsrechtlichen Vorgaben genügen. Die Verfassungsmäßigkeit der §§ 184b, 184c LVwGE lässt sich indes ebenfalls mit vertretbarer Begründung bejahen. Der Landesgesetzgeber muss daher entscheiden, ob er trotz der verfassungsrechtlichen Risiken an den §§ 184b, 184c LVwGE festhalten möchte.

Begrüßenswert ist hingegen, dass nach § 184c Abs. 1 Satz 2 LVwGE das Ergebnis des Abgleichs durch zwei qualifizierte Beschäftigte der Polizei zu überprüfen und zu bestätigen ist, bevor weitere polizeiliche Maßnahmen getroffen werden. Das Vier-Augen-Prinzip ist geeignet, die Fehleranfälligkeit und damit das Eingriffsgewicht der biometrischen Echtzeit-Fernidentifizierung zu reduzieren. Gleiches gilt für das Erfordernis einer besonderen Qualifikation der Beschäftigten der Polizei.

Im Übrigen fehlt es auch im Hinblick auf die Echtzeit-Fernidentifizierung gemäß §§ 184b, 184c LVwGE an besonderen verfahrensrechtlichen Vorkehrungen zur Verringerung der Fehleranfälligkeit der eingesetzten Systeme sowie an Regelungen zur Sicherung digitaler Souveränität. Es empfiehlt sich, entsprechende Bestimmungen in den Gesetzesentwurf aufzunehmen. Zur Vermeidung unnötiger Wiederholungen wird auf die Ausführungen unter II. 2. und II. 3. verwiesen.

³⁸ Heckmann/Klauser/Ziegler, LT-Umdruck 20/6959, S. 15.

³⁹ Heckmann/Klauser/Ziegler, LT-Umdruck 20/6959, S. 15 f.

⁴⁰ LT-Drs. 20/6959, S. 45.

⁴¹ Vgl. BVerfG, Urteil vom 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 Rn. 100.

IV. Nachträgliche Fernidentifizierung, §§ 195b, 195c LVwGE

§§ 195b, 195c LVwGE ermächtigen die Polizei zur nachträglichen Fernidentifizierung. Die nachträgliche Fernidentifizierung erfolgt durch einen Abgleich polizeilicher Daten mit Daten, die aus dem öffentlich zugänglichen Bereich des Internets erlangt wurden. Hiervon umfasst sind auch Daten aus sozialen Medien. Die Regelungen der §§ 195b, 195c LVwGE müssen unionsrechtlichen sowie verfassungsrechtlichen Anforderungen genügen.

1. Vorgaben der KI-Verordnung

Gemäß Art. 5 Abs. 1 Buchst. e KI-VO ist die Verwendung von KI-Systemen, die Datenbanken zur Gesichtserkennung durch das ungezielte Auslesen von Gesichtsbildern aus dem Internet oder von Überwachungsaufnahmen erstellen oder erweitern, verboten. Die Bedeutung des Begriffs „ungezieltes Auslesen“ ist bislang nicht abschließend geklärt. In der Begründung des Gesetzesentwurfs heißt es hierzu, ein ungezieltes Auslesen liege nicht vor, sofern Gesichtsbilder nur anlassbezogen gewonnen werden und nur für diesen Anlass verarbeitet würden.⁴² Hingegen vertritt die EU-Kommission in ihren – rechtlich nicht verbindlichen – Leitlinien die Auffassung, ein Auslesen sei nur dann „ungezielt“, wenn es einen spezifischen Fokus auf eine bestimmte Person oder Personengruppe lege.⁴³ Demnach wäre auch der anlassbezogene Aufbau einer Datenbank durch das Auslesen von Gesichtsbildern mithilfe von KI-Systemen gemäß Art. 5 Abs. 1 Buchst. e KI-VO verboten.

Nach einem Gutachten von *Lewandowski* ist die technische Umsetzbarkeit eines Abgleichs mit öffentlich zugänglichen Daten aus dem Internet ohne den Aufbau einer Datenbank nicht möglich.⁴⁴ Hieraus wird teilweise gefolgert, dass Art. 5 Abs. 1 Buchst. e KI-VO einer nachträglichen biometrischen Fernidentifizierung anhand von Gesichtsdaten entgegenstehe.⁴⁵ Allerdings ist eine solche Schlussfolgerung nicht zwingend. Das Verbot des Art. 5 Abs. 1 Buchst. e KI-VO bezieht sich lediglich auf solche Datenbanken, die

⁴² LT-Drs. 20/4284, S. 59.

⁴³ European Commission, Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), C(2025) 5052 final Rn. 228.

⁴⁴ *Lewandowski*, Braucht die Polizei eine Datenbank zum biometrischen Abgleich? Das Durchsuchen von Internetbildern zur Gesichtserkennung, abrufbar unter: <https://algorithmwatch.org/de/gutachten-datenbank-biometrie-gesichtserkennung/> (Abruf: 05.09.2026).

⁴⁵ Vgl. *Heckmann/Klauser/Ziegler*, LT-Umdruck 20/6959, S. 15 f.

mithilfe von KI-Systemen generiert wurden.⁴⁶ Hingegen fallen Datenbanken, die durch einen fest vorgegebenen, menschlich definierten Algorithmus erzeugt werden, nicht in den Anwendungsbereich der Verbotsnorm.⁴⁷ Entscheidend ist mithin, dass für das Erstellen der Datenbank kein KI-System im Sinne von Art. 3 Nr. 1 KI-VO verwendet wird. Dies sollte in § 195b LVwGE ausdrücklich festgeschrieben werden. Insgesamt spricht einiges dafür, dass die §§ 195b, 195c LVwGE mit der KI-Verordnung vereinbar sind.

Bei der praktischen Anwendung der §§ 195b, 195c LVwGE müssen zudem die Anforderungen der KI-Verordnung an Hochrisiko-KI-Systeme (vgl. Art. 9 ff. KI-VO) beachtet werden. Insoweit sei auf die Ausführungen unter III. 1. verwiesen.

2. Verfassungsrechtliche Anforderungen

Als schwerwiegender Eingriff in das Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) unterliegt die nachträgliche Fernidentifizierung gemäß §§ 195b, 195c LVwGE besonders strengen verfassungsrechtlichen Anforderungen. Da es bislang an einer Entscheidung des Bundesverfassungsgerichts zur Zulässigkeit der nachträglichen biometrischen Fernidentifizierung fehlt, sind die genauen Anforderungen unklar. Die Begründung des Gesetzesentwurfs geht davon aus, dass die Grundsätze des Bundesverfassungsgerichts zur Rasterfahndung für eine Fernidentifizierung, die sich des Internets als Datenquelle bedient, entsprechend gelten.⁴⁸ Sollte dies zutreffen, wären die §§ 195b, 195c LVwGE verfassungsgemäß.

Eine Übertragung der Grundsätze zur Rasterfahndung ist jedoch nicht zwingend: Die nachträgliche Fernidentifizierung, insbesondere mithilfe von künstlicher Intelligenz, hat eine erhebliche Streubreite und betrifft eine Vielzahl – auch sensibler – Daten. Aufgrund der Fähigkeit selbstlernender Systeme, umfangreiche Datenmengen binnen kurzer Zeit auszuwerten, ist die Maßnahme wesentlich effektiver als eine herkömmliche Rasterfahndung. Daher hat sie zugleich eine höhere Eingriffsintensität. Das Bundesverfassungsgericht hat in seiner Entscheidung zur automatisierten Datenanalyse ausgeführt, dass der Einsatz von KI-Systemen das Eingriffsgewicht einer Maßnahme erhöhen kann.⁴⁹ Insgesamt bestehen Zweifel, ob die §§ 195b, 195c LVwGE den verfassungsrechtlichen

⁴⁶ Hahn, Verfassungsblog vom 31.03.2026.

⁴⁷ Hahn, Verfassungsblog vom 31.03.2026.

⁴⁸ LT-Drs. 20/4284, S. 58.

⁴⁹ Vgl. BVerfG, Urteil vom 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20, NJW 2023, 1196 Rn. 100.

Anforderungen genügen.⁵⁰ Die Verfassungsmäßigkeit der §§ 195b, 195c LVwGE lässt sich indes ebenfalls mit vertretbarer Begründung bejahen. Der Landesgesetzgeber muss daher entscheiden, ob er trotz der verfassungsrechtlichen Risiken an den §§ 195b, 195c LVwGE festhalten möchte.

Begrüßenswert ist demgegenüber, dass nach § 195c Abs. 1 Satz 2 LVwGE das Ergebnis eines Abgleichs, bevor weitere polizeiliche Maßnahmen getroffen werden, durch zwei Beschäftigte der Polizei zu überprüfen und zu bestätigen ist. Allerdings beschränkt § 195c Abs. 1 Satz 2 LVwGE die Überprüfung nicht auf qualifizierte Beschäftigte der Polizei. Besondere Qualifikationen sind gemäß § 195c Abs. 3 Satz 1 LVwGE lediglich für den Zugang zu der Anwendung, mit der die Maßnahme umgesetzt wird, erforderlich. Nur qualifizierte Beschäftigte sind indes in der Lage, das Ergebnis einer nachträglichen Fernidentifizierung sachgerecht zu kontrollieren. Daher sollte § 195c Abs. 1 Satz 2 LVwGE um eine Regelung ergänzt werden, wonach ausschließlich qualifizierte Beschäftigte der Polizei das Ergebnis des Abgleichs überprüfen dürfen.

Überdies fehlt es auch im Hinblick auf die nachträgliche Fernidentifizierung gemäß §§ 195b, 195c LVwGE an besonderen verfahrensrechtlichen Vorkehrungen zur Verringerung der Fehleranfälligkeit der eingesetzten Systeme sowie an Regelungen zur Sicherung digitaler Souveränität. Es empfiehlt sich, entsprechende Bestimmungen in den Gesetzesentwurf aufzunehmen. Zur Vermeidung unnötiger Wiederholungen wird auf die Ausführungen unter II. 2. und II. 3. verwiesen.

V. Gewahrsam von Personen, §§ 204, 205, 205a LVwGE

Die Regelungen zum Gewahrsam von Personen (§§ 204, 205, 205a LVwGE) werfen rechtliche Fragen auf, insbesondere im Hinblick auf die Höchstdauer des Gewahrsams nach § 204 Abs. 6 Satz 2 LVwGE und den Gewahrsam für Begleitpersonen nach § 204 Abs. 1 Nr. 2 Halbsatz 2 Buchst. b LVwGE.

⁵⁰ Vgl. *Heckmann/Klauser/Ziegler*, LT-Umdruck 20/6959, S. 21.

1. Zur Höchstdauer des Gewahrsams, § 204 Abs. 6 Satz 2 LVwGE

In § 204 Abs. 6 Satz 2 LVwGE legt der schleswig-holsteinische Landesgesetzgeber erstmals eine gesetzliche Höchstdauer des Gewahrsams fest. Beruht der Gewahrsam auf einer richterlichen Entscheidung, hat diese nach § 204 Abs. 6 Satz 1 LVwGE die höchstzulässige Dauer der Freiheitsentziehung zu bestimmen. Sie darf gemäß § 204 Abs. 6 Satz 2 LVwGE jeweils nicht mehr als einen Monat betragen und kann insgesamt nur bis zu einer Gesamtdauer von zwei Monaten verlängert werden.

Grundsätzlich ist es begrüßenswert, dass § 204 Abs. 6 Satz 2 LVwGE eine Höchstdauer für den Gewahrsam vorgibt. Hierdurch schafft der Landesgesetzgeber ein höheres Maß an Normbestimmtheit und Rechtssicherheit für die Praxis. Eine Gewahrsamshöchstdauer von zwei Monaten stößt jedoch auf verfassungsrechtliche Bedenken. Die Bestimmung des § 204 Abs. 6 Satz 2 LVwGE ist angelehnt an die Regelung in Art. 20 Abs. 2 Satz 2 BayPAG. Gegen diese Bestimmung ist derzeit ein Verfahren vor dem BVerfG anhängig; die mündliche Verhandlung fand am 07.07.2026 statt.⁵¹ Der Ausgang des Verfahrens kann hier nicht vorweggenommen werden.

Es spricht indes einiges dafür, dass eine Höchstdauer des Gewahrsams von zwei Monaten unverhältnismäßig ist und gegen Art. 2 Abs. 2 Satz 2 GG i.V.m. Art. 104 Abs. 2 Satz 3 GG verstößt. Als besonders schwerwiegender Eingriff ist der Gewahrsam nur so lange zulässig, bis andere, weniger eingreifende Mittel zum Schutz des gefährdeten Rechtsguts zur Verfügung stehen und damit der Grund der Maßnahme weggefallen ist.⁵² Nach Ansicht von *Gusy* und *Eichenhofer* ist dies regelmäßig am Abend des nächsten Tages, spätestens nach vier Tagen, in jedem Falle aber vor dem Ablauf von zwei Wochen der Fall.⁵³

Das Bundesverfassungsgericht hat in einer Entscheidung zur nachträglichen Sicherungsverwahrung ausgeführt, die längerfristige Verwahrung einer psychisch gesunden und strafrechtlich nicht oder nur unerheblich vorbelasteten Person zum Zweck der Abwehr einer von ihr ausgehenden Gefahr der Begehung von Straftaten sei mit dem Grundgesetz nicht vereinbar.⁵⁴ In diesem Zusammenhang bezeichnet das Bundesverfassungsgericht den „bis zu 14-tägige[n] landesrechtliche[n] Polizeigewahrsam“ als „situationsbezogene[s] Instrument“, mit dem der Staat auf konkrete Gefahrensituationen reagieren

⁵¹ Siehe hierzu *Bonn*, JuWissBlog vom 29.07.2026.

⁵² *Gusy/Eichenhofer*, Polizei- und Ordnungsrecht, 11. Aufl. 2023, Rn. 308.

⁵³ *Gusy/Eichenhofer*, Polizei- und Ordnungsrecht, 11. Aufl. 2023, Rn. 308.

⁵⁴ BVerfG, Urteil vom 10.02.2004 – 2 BvR 834, 1588/02, BVerfGE 109, 190 (220).

dürfe.⁵⁵ Zwar lässt sich aus dieser Aussage des Bundesverfassungsgerichts nicht ableiten, dass für den Polizeigewahrsam allgemein eine verfassungsrechtliche Höchstfrist von 14 Tagen gilt.⁵⁶ Die Ausführungen des Bundesverfassungsgerichts verdeutlichen aber, dass der Polizeigewahrsam einen Bezug zu einer konkreten Gefahrensituation aufweisen muss. Dieser Situationsbezug begrenzt die Dauer des Polizeigewahrsams: Je länger der Polizeigewahrsam andauert, desto lockerer ist der Bezug zu der gewahrsamsauslösenden Gefahrensituation und desto strenger sind die Anforderungen an die verfassungsrechtliche Rechtfertigung des Polizeigewahrsams.⁵⁷

Der BayVerfGH hat die Bestimmung des Art. 20 Abs. 2 Satz 2 BayPAG als mit dem Grundrecht der Freiheit der Person nach Art. 101 Abs. 1 BV vereinbar angesehen.⁵⁸ Die Regelung des Art. 20 Abs. 2 Satz 2 BayPAG gelte nur für Fälle, in denen der Gewahrsamsgrund nicht weggefallen sei, mithin nur bei noch andauernder Gefahrenlage.⁵⁹ Dies zugrunde gelegt, enthalte Art. 20 Abs. 2 Satz 2 BayPAG keinen unverhältnismäßigen Eingriff in das Freiheitsgrundrecht des Art. 102 BV.⁶⁰ Die Anordnung einer polizeilichen Ingewahrsamnahme sei nur als letztes Mittel zugelassen, wenn zur Gefahrenabwehr kein anderes, weniger belastendes Mittel ausreiche. Zudem sei die Ausschöpfung der Höchstfrist nicht zwingend vorgegeben; vielmehr werde die Dauer des Gewahrsams im Einzelfall von einem unabhängigen Richter unter Berücksichtigung der Umstände des jeweiligen Einzelfalls, insbesondere des Gewahrsamsgrunds, festgelegt. Darüber hinaus sei die Fortdauer des Gewahrsams an die Fortdauer des jeweiligen Gewahrsamsgrunds geknüpft, weshalb eine Gewahrsamshöchstdauer von zwei Monaten nur in Ausnahmefällen in Betracht komme.⁶¹

Zweifelhaft ist allerdings, ob überhaupt Fälle denkbar sind, in denen ein Gewahrsamsgrund über eine Dauer von zwei Monaten fortbesteht.⁶² *Poscher* und *Werner* argumentieren, es sei „für keines der Schutzgüter des Gewahrsams [...] erforderlich, dass sich dieser sich über mehr als wenige Tage erstreckt“. ⁶³ Während eines mehrtägigen Gewahrsams sei es möglich, mildere Maßnahmen, wie etwa solche zur Aufenthaltsüberwachung oder Observation, bereitzustellen.⁶⁴ Zudem lasse sich während eines Zeitraums von 30 oder gar

⁵⁵ BVerfG, Urteil vom 10.02.2004 – 2 BvR 834, 1588/02, BVerfGE 109, 190 (220).

⁵⁶ Vgl. BayVerfGH, Entscheidung vom 14.06.2023 – Vf. 15–VII–18, GSZ 2023, 190 Rn. 160 ff.

⁵⁷ Vgl. BVerfG, Urteil vom 05.02.2004 – 2 BvR 2029/01, BVerfGE 109, 133 (159); BayVerfGH, Entscheidung vom 14.06.2023 – Vf. 15–VII–18, GSZ 2023, 190 Rn. 138.

⁵⁸ BayVerfGH, Entscheidung vom 14.06.2023 – Vf. 15–VII–18, GSZ 2023, 190 Rn. 125 ff.

⁵⁹ BayVerfGH, Entscheidung vom 14.06.2023 – Vf. 15–VII–18, GSZ 2023, 190 Rn. 128.

⁶⁰ BayVerfGH, Entscheidung vom 14.06.2023 – Vf. 15–VII–18, GSZ 2023, 190 Rn. 137 ff.

⁶¹ BayVerfGH, Entscheidung vom 14.06.2023 – Vf. 15–VII–18, GSZ 2023, 190 Rn. 157.

⁶² Vgl. *Bonn*, JuWissBlog vom 29.07.2026; *Meiertöns*, GSZ 2023, 199 (201 f.).

⁶³ *Poscher/Werner*, Verfassungsblog vom 24.11.2022.

⁶⁴ *Poscher/Werner*, Verfassungsblog vom 24.11.2022.

60 Tagen keine solche zeitliche Nähe des befürchteten Schadenseintritts bejahen, dass die Freiheitsentziehung noch in angemessenem Verhältnis zu dem mit ihr bezweckten Ziel stehe.⁶⁵

Selbst wenn das Bundesverfassungsgericht eine Gewahrsamshöchstdauer von zwei Monaten als verfassungsgemäß ansehen sollte, wären praktisch kaum Fälle denkbar, in denen eine derartige Gewahrsamshöchstdauer verhältnismäßig wäre. Dementsprechend haben andere Länder bislang kein Bedürfnis gesehen, eine an Art. 20 Abs. 2 Satz 2 BayPAG angelehnte Regelung zu schaffen. Derzeit ist Bayern das einzige Land, das eine Gewahrsamshöchstdauer von zwei Monaten vorsieht. Die Polizeigesetze anderer Länder enthalten teils wesentlich restriktivere Regelungen. So gilt für den Polizeigewahrsam in Hamburg eine Höchstdauer von zehn Tagen (vgl. § 13c Abs. 1 Nr. 3 Satz 2 Halbsatz 3 HmbSOG), in Baden-Württemberg und Sachsen eine Höchstdauer von zwei Wochen (vgl. § 33 Abs. 3 Satz 5 BWPoIG; § 26 Nr. 3 Halbsatz 3 SächsPVDG).

Insgesamt ist unsicher, ob eine Gewahrsamshöchstdauer von zwei Monaten mit Art. 2 Abs. 2 Satz 2 GG i.V.m. Art. 104 Abs. 2 Satz 3 GG vereinbar wäre. Hingegen wäre eine Gewahrsamshöchstdauer von zwei Wochen verfassungsrechtlich unbedenklich. Daher sollte die Höchstdauer des Gewahrsams auf zwei Wochen verkürzt werden. Hierbei könnte sich der Landesgesetzgeber an der Regelung in Baden-Württemberg (vgl. § 33 Abs. 3 Satz 5 BWPoIG) orientieren. Es empfiehlt sich folgende Formulierung des § 204 Abs. 6 LVwGE:

„Beruht der Gewahrsam auf einer richterlichen Entscheidung, hat diese die höchstzulässige Dauer der Freiheitsentziehung zu bestimmen. Sie darf nicht mehr als zwei Wochen betragen.“

2. Zum Gewahrsam für Begleitpersonen, § 204 Abs. 1 Nr. 2 Halbsatz 2 Buchst. b LVwGE

Nach § 204 Abs. 1 Nr. 2 Halbsatz 1 LVwGE kann die Polizei eine Person in Gewahrsam nehmen, wenn dies unerlässlich ist, um die unmittelbar bevorstehende Begehung oder Fortsetzung einer Ordnungswidrigkeit von erheblicher Bedeutung für die Allgemeinheit oder einer Straftat zu verhindern. Die Annahme der Begehung oder Fortsetzung einer Tat im Sinne des Halbsatzes 1 kann sich gemäß § 204 Abs. 1 Nr. 2 Halbsatz 2 Buchst. b

⁶⁵ Poscher/Werner, Verfassungsblog vom 24.11.2022.

LVwGE insbesondere darauf stützen, dass bei der Person Waffen, Werkzeuge oder sonstige Gegenstände aufgefunden werden und Tatsachen die Annahme rechtfertigen, dass diese Gegenstände zur Begehung der Tat bestimmt sind, oder ihre Begleitperson solche Gegenstände mit sich führt und sie den Umständen nach hiervon Kenntnis haben musste. Ausweislich der Gesetzesbegründung stellen die legislativen Prognosehilfen keine Regelbeispiele, sondern lediglich Auslegungshilfen dar.⁶⁶ Die Bestimmung des § 204 Abs. 1 Nr. 2 Halbsatz 2 Buchst. b LVwGE ist an vergleichbare Regelungen in anderen Ländern angelehnt (siehe etwa Art. 17 Abs. 1 Nr. 2 Buchst. b BayPAG; § 17 Abs. 1 Nr. 2 Buchst. b BbgPolG; § 55 Abs. 1 Nr. 2 Buchst. b SOG M-V).

Es stellt sich die Frage, ob der Umstand, dass eine Begleitperson gefährliche Gegenstände mit sich führt und eine Person den Umständen nach hiervon Kenntnis haben musste, eine hinreichende Gefahrenprognose für eine Ingewahrsamnahme begründen kann. Diese Frage betrifft allerdings nicht die Verfassungskonformität des § 204 Abs. 1 Nr. 2 Halbsatz 2 Buchst. b LVwGE, sondern seine Anwendung im Einzelfall. Die Möglichkeit eines Gewahrsams für Begleitpersonen gemäß § 204 Abs. 1 Nr. 2 Halbsatz 2 Buchst. b LVwGE ist einer verfassungskonformen Anwendung zugänglich. Es ist nicht von vornherein ausgeschlossen, dass die Begleitung einer Person, die erkennbar gefährliche Gegenstände mit sich führt, in bestimmten Fällen die Annahme rechtfertigen kann, dass eine Person eine Ordnungswidrigkeit von erheblicher Bedeutung für die Allgemeinheit oder einer Straftat begehen wird. Allerdings sind an eine derartige Gefahrenprognose strenge Anforderungen zu stellen. Die bloße Begleitung einer Person, die gefährliche Gegenstände mit sich führt, darf – zumal angesichts der Eingriffsintensität des polizeilichen Gewahrsams – nicht zu einer Mithaftung führen.

VI. Maßnahmen gegen unbemannte Fahrzeugsysteme, § 213a LVwGE

§ 213a LVwGE ermächtigt die Polizei zu Maßnahmen gegen unbemannte Fahrzeugsysteme. Derartige Maßnahmen sind bislang auf der Grundlage der polizeilichen Generalklausel (§§ 174, 176 Abs. 1 LVwGE) möglich. Es ist begrüßenswert, dass der Landesgesetzgeber nunmehr eine eigene Standardermächtigung für die Drohnenabwehr schafft. Damit trägt der Landesgesetzgeber dem Umstand Rechnung, dass Maßnahmen gegen unbemannte

⁶⁶ LT-Drs. 20/4284, S. 34.

Fahrzeugsysteme in der polizeilichen Praxis häufiger notwendig werden.⁶⁷ Zudem erhöht eine spezifische Rechtsgrundlage die Bestimmtheit und Rechtssicherheit für die polizeiliche Praxis.

Vergleichbare gesetzliche Regelungen zur Drohnenabwehr existieren bereits in Hessen (§ 15e HSOG), Rheinland-Pfalz (§ 9b POG RhPf) und Bayern (Art. 29a BayPAG). In der Literatur ist allerdings umstritten, ob dem Landesgesetzgeber für die Regelung von Maßnahmen zur Drohnenabwehr eine Gesetzgebungskompetenz zusteht. *Thiel* und *Probst* vertreten die Auffassung, für gesetzliche Regelungen zur Abwehr von Drohnen bestehe eine Annexkompetenz des Bundes zur ausschließlichen Gesetzgebungskompetenz gemäß Art. 73 Abs. 1 Nr. 6 GG („Luftverkehr“), die ihrerseits ausschließlichen Charakter habe.⁶⁸ Landesgesetzliche Ermächtigungsnormen zum Einsatz technischer Mittel gegen unbemannte Luftfahrtsysteme seien daher formell verfassungswidrig.⁶⁹ Demgegenüber nehmen *Becker* und *Gräber* an, dass für den Erlass von Maßnahmen zur Drohnenabwehr grundsätzlich die Länder zuständig seien (Art. 30, 70 GG).⁷⁰

Letztere Auffassung ist überzeugend. Nach Art. 30, 70 GG fällt die Gefahrenabwehr grundsätzlich in den Zuständigkeitsbereich der Länder. Eine Annexkompetenz des Bundes ist in der föderalen Kompetenzordnung eine rechtfertigungsbedürftige Ausnahme. Sie setzt voraus, dass ein Sachbereich mit einem Sachgebiet, für das der Bund die Gesetzgebungskompetenz hat, in einem notwendigen Zusammenhang stehen.⁷¹ Die ausschließliche Gesetzgebungskompetenz des Bundes für den Luftverkehr gemäß Art. 73 Abs. 1 Nr. 6 GG umfasst alle mit dem Flugwesen zusammenhängenden Tätigkeiten und Institutionen.⁷² Auch die Gesetzgebungszuständigkeit für Maßnahmen der Gefahrenabwehr lässt sich als Annexkompetenz auf Art. 73 Abs. 1 Nr. 6 GG stützen.⁷³ Dies gilt jedoch nur insoweit, als die Maßnahmen mit dem Luftverkehr in einem funktionalen Zusammenhang stehen, weil sie der Abwehr luftverkehrsspezifischer Gefahren dienen.⁷⁴ Der Annexkompetenz zu Art. 73 Abs. 1 Nr. 6 GG liegt der Gedanke zugrunde, dass eine dezentrale Regelungszuständigkeit zu unzureichend abwehrwirksamen Regelungen eines einzelnen Landes führen könnte, deren negative Folgen nicht auf das betreffende Land beschränkt wären.⁷⁵ Diese Voraussetzungen sind bei der Drohnenabwehr nicht

⁶⁷ Vgl. *Thiel/Probst*, KriPoZ 2025, 403 (404).

⁶⁸ *Thiel/Probst*, KriPoZ 2025, 403 (410).

⁶⁹ *Thiel/Probst*, KriPoZ 2025, 403 (410).

⁷⁰ *Becker/Gräber*, NVwZ 2025, 1860 (1860).

⁷¹ Vgl. BVerfG, Beschluss vom 03.07.2012 – 2 PBvU 1/11, NVwZ 2012, 1239 Rn. 17.

⁷² *Seiler*, in: BeckOK GG, 65. Ed. 01.03.2026, GG Art. 73 Rn. 25.

⁷³ Vgl. BVerfG, Beschluss vom 03.07.2012 – 2 PBvU 1/11, NVwZ 2012, 1239 Rn. 17 f.

⁷⁴ Vgl. BVerfG, Beschluss vom 03.07.2012 – 2 PBvU 1/11, NVwZ 2012, 1239 Rn. 18 f.; LT-Umdruck 20/6786, S. 64 f. m.w.N.

⁷⁵ BVerfG, Beschluss vom 03.07.2012 – 2 PBvU 1/11, NVwZ 2012, 1239 Rn. 19.

erfüllt; insbesondere drohen durch unbemannte Fahrzeugsysteme keine katastrophenhaften Sachlagen im Sinne von Art. 35 Abs. 2 Satz 2 und Abs. 3 GG.⁷⁶ Daher ist es nicht geboten, die Drohnenabwehr in die Annexkompetenz des Bundes für den Luftverkehr einzubeziehen. Die Bestimmung des § 213a LVwGE ist von der Gesetzgebungszuständigkeit des Landes gedeckt.

VII. Zusammenfassung

Der Gesetzesentwurf dehnt die Befugnisse der Landespolizei erheblich aus. Das Bestreben des Gesetzgebers, die eingriffsintensiven Maßnahmen rechtsstaatlich einzuhegen, ist deutlich erkennbar. Einige Regelungen stoßen gleichwohl auf verfassungsrechtliche Bedenken. Im Einzelnen empfehlen sich folgende Änderungen:

1. Die Ermächtigung zur Erstellung eines Verhaltensprofils in § 188c Abs. 7 LVwGE sollte auf die Datenanalyse mit hohem Eingriffsgewicht (§ 188c Abs. 4 LVwGE) beschränkt werden.
2. Die Bestimmungen zur automatisierten Datenanalyse in §§ 188c, 188d LVwGE sowie die Bestimmungen zur Fernidentifizierung in §§ 184b, 184c LVwGE und §§ 195b, 195c LVwGE sollten um verfahrensrechtliche Vorkehrungen ergänzt werden. Diese sollten insbesondere Regelungen zur Gewährleistung einer hinreichenden Datenqualität sowie zur regelmäßigen Überprüfung der verwendeten Systeme umfassen.
3. Zudem sollten die Bestimmungen zur automatisierten Datenanalyse in §§ 188c, 188d LVwGE sowie die Bestimmungen zur Fernidentifizierung in §§ 184b, 184c LVwGE und §§ 195b, 195c LVwGE um Regelungen zur Sicherung digitaler Souveränität ergänzt werden. Insbesondere sollte ein Vorrang von Eigenentwicklungen und Open-Source-Komponenten sowie Software aus der Europäischen Union gesetzlich festgeschrieben werden.
4. In § 195b LVwGE sollte ausdrücklich festgelegt werden, dass für das Erstellen oder Erweitern einer Datenbank zur Gesichtserkennung kein KI-System im Sinne von Art. 3 Nr. 1 KI-VO verwendet werden darf.

⁷⁶ Vgl. LT-Umdruck 20/6786, S. 66.

5. § 195c Abs. 1 Satz 2 LVwGE sollte um eine Regelung ergänzt werden, wonach ausschließlich qualifizierte Beschäftigte der Polizei das Ergebnis des Abgleichs überprüfen dürfen.
6. Die Höchstdauer des Gewahrsams in § 204 Abs. 6 LVwGE sollte auf zwei Wochen verkürzt werden.

Darüber hinaus sollte der Landesgesetzgeber überdenken, ob er trotz verfassungsrechtlicher Risiken aufgrund der hohen Eingriffsintensität an den Bestimmungen zur Fernidentifizierung in §§ 184b, 184c LVwGE und §§ 195b, 195c LVwGE festhalten möchte.

Für Rückfragen stehe ich Ihnen jederzeit gern zur Verfügung.

Mit freundlichen Grüßen

Dr. Simon Diethelm Meyer