

Univ.-Prof. Dr. Dr. Markus Thiel

Deutsche Hochschule der Polizei

Fachgebiet III.4 – Öffentliches Recht mit Schwerpunkt Polizeirecht

An den
Schleswig-Holsteinischen Landtag
Herrn Abg. Jan Kürschner
Vorsitzender des Innen- und Rechtsausschusses
Düsternbrocker Weg 70

24105 Kiel

Stellungnahme

zum Gesetzentwurf der Landesregierung – Ministerin für Inneres, Kommunales, Wohnen und Sport „Gesetz zur Fortentwicklung polizeirechtlicher Maßnahmen für einen wirksamen Schutz der öffentlichen Sicherheit“, LT-Drs. 20/4284 v. 24. März 2026,

zum Änderungsantrag der Fraktionen der CDU und BÜNDNIS 90/DIE GRÜNEN zur Drucksache 20/4284, Umdruck 20/6786 v. 6. Juli 2026

A. Gegenstand der Stellungnahme

Mit Schreiben des Vorsitzenden des Innen- und Rechtsausschusses des Schleswig-Holsteinischen Landtags vom 25. Juni 2026 wurde die Deutsche Hochschule der Polizei um Abgabe einer Stellungnahme zum Gesetzentwurf der Landesregierung – Ministerin für Inneres, Kommunales, Wohnen und Sport – „Gesetz zur Fortentwicklung polizeirechtlicher Maßnahmen für einen wirksamen Schutz der öffentlichen Sicherheit“ vom 24. März 2026 (LT-Drs. 20/4284) gebeten. Mit Schreiben vom 10. Juli 2026 erfolgt eine Bitte zur Berücksichtigung des Änderungsantrags der Fraktionen von CDU und BÜNDNIS 90/DIE GRÜNEN vom 6. Juli 2026 (Umdruck 20/6786).

Der Unterzeichner als Leiter des Fachgebiets III.4 – Öffentliches Recht mit Schwerpunkt Polizeirecht – hat die Erarbeitung der Stellungnahme übernommen. Die nachstehenden Ausführungen geben die persönliche Auffassung des Unterzeichners wieder und beschränken sich angesichts des Umfangs des Gesetzentwurfs und des Änderungsantrags

auf ausgewählte Aspekte. Verwiesen wird auf die vom Unterzeichner bereits im Rahmen der Verbändeanhörung erstellte Stellungnahme vom 7. November 2025.

B. Rechtliche Würdigung

I. Allgemeines

Der Gesetzentwurf beabsichtigt – wie schon die im Rahmen der Verbändeanhörung vorgelegte Fassung – eine umfassende Anpassung und Ergänzung des Allgemeinen Verwaltungsgesetzes für das Land Schleswig-Holstein (Landesverwaltungsgesetz – LVwG), in dem sich die wesentlichen polizeirechtlichen Vorschriften finden (§§ 162 ff. LVwG).

Ausweislich der Begründung des Gesetzentwurfs ist wesentlicher Anlass das Anwachsen von „Messerangriffen“ in der Öffentlichkeit. Dazu werden einige Bestimmungen des Gesetzes zur Erhebung und zum Abgleich von Daten modifiziert und durch weitere Vorschriften flankiert. Insbesondere soll der Einsatz technischer Weiterentwicklungen ermöglicht werden. Namentlich die Regelungen zum Datenabgleich werden durch zwei neuartige Instrumente erweitert: Zum einen durch die automatisierte Datenanalyse, zum anderen durch die biometrische Fernidentifizierung in zwei Varianten (Echtzeit- und nachträgliche Fernidentifizierung). Die Ermächtigungsnorm für die Videoüberwachung des öffentlichen Raums soll ausgeweitet werden. Ebenfalls neu gefasst werden sollen – zur Schließung von „Schutzlücken“ – die Vorschriften zum Präventivgewahrsam und zur elektronischen Aufenthaltsüberwachung. Die genannten fünf Maßnahmen sind Gegenstand der nachfolgenden Ausführungen, wobei nicht alle der differenzierten und detailreichen Einzelregelungen behandelt werden können. Die im Änderungsantrag vorgeschlagenen Anpassungen werden dabei berücksichtigt; auf eine Auswahl der dort vorgeschlagenen zusätzlichen Regelungen wird im Anschluss kurz eingegangen.

II. Videoüberwachung des öffentlichen Raums (Datenerhebung bei öffentlichen Veranstaltungen und Ansammlungen sowie in allgemein zugänglichen Orten)

§ 184 LVwG-E sieht eine Neufassung der Ermächtigungsgrundlage für die Datenerhebung bei öffentlichen Veranstaltungen und Ansammlungen sowie auf öffentlichen Flächen vor. Die Vorschrift unterscheidet in den Absätzen 1 – 4 verschiedene zulässige Maßnahmen: Ansatz 1 erlaubt die Erhebung personenbezogener Daten bei oder im

Zusammenhang mit öffentlichen Veranstaltungen und Ansammlungen, die nicht dem Versammlungsgesetz unterliegen. Für den offenen Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufnahmen beschränkt die Norm den zulässigen Adressatenkreis auf die in §§ 218, 219 LVwG genannten Personen. Die vorgesehene Eingriffsschwelle erscheint sachgerecht – die Norm knüpft an Tatsachen an, die dafür sprechen, dass von den Betroffenen Ordnungswidrigkeiten von erheblicher Bedeutung oder Straftaten begangen werden.

Absatz 2 normiert die „Live“-Beobachtung allgemein zugänglicher Flächen mittels Bildübertragung (Satz 1) sowie die entsprechende Beobachtung von Räumen, die nicht der Wohnung dienen, und auf befriedetem Besitztum, jeweils zu einer Zeit, da Raum bzw. Besitztum bestimmungsgemäß für die Allgemeinheit geöffnet sind. Tatbestandlich angeknüpft werden die Maßnahmen (lediglich) an die Aufgabenerfüllung nach § 162 LVwG (insbesondere Gefahrenabwehr), so dass die Eingriffsschwelle minimal niedrig angesetzt ist. Dies erscheint im Hinblick darauf, dass es sich lediglich um eine Bildübertragung ohne Aufzeichnung handelt und die zulässigen Zielorte nach verfassungsrechtlichen Kriterien in erheblicher Weise eingegrenzt werden, als vertretbar.

Gemäß Absatz 3 sollen offene Bild- und Tonaufnahmen oder -aufzeichnungen von Personen auf und an allgemein zugänglichen Flächen bzw. in Räumen und auf befriedetem Besitztum i.S.v. Absatz 2 Satz 2 zulässig sein, wenn dies zur Abwehr einer Gefahr für die öffentliche Sicherheit erforderlich ist (Nr. 1), Tatsachen die Annahme rechtfertigen, dass an dem Ort Ordnungswidrigkeiten von erheblicher Bedeutung oder Straftaten begangen werden (Nr. 2), oder es sich um Orte im Sinne des § 181 Abs. 1 Nr. 1 – 3 LVwG handelt (Nr. 3; gefährdete Orte und Objekte, dort Aufnahmen und Aufzeichnungen nur durch die Polizei erlaubt). Diese örtliche Anbindung stellt gegenüber der aktuell geltenden Regelung durchaus eine Ausweitung dar, geht es doch in § 184 Abs. 2 S. 1 LVwG bislang (nur) um Kriminalitäts- und Gefahrenschwerpunkte. Die vorgeschlagene Neufassung begegnet angesichts der weiteren normativen Beschränkungen und der tatbestandlich ausdifferenzierten Varianten keinen Bedenken und ist aus praktischer Perspektive zu begrüßen, weil insbesondere kritische und besonders gefährdete Infrastruktur in die Beobachtung einbezogen werden kann. Eine „flächendeckende“ Überwachung ist gleichwohl nicht zu befürchten, wenngleich zuzugestehen ist, dass die drei tatbestandlichen Varianten einen vergleichsweise weit gefassten Anwendungsbereich eröffnen.

Die Vorschrift enthält weitere Einschränkungen (räumliche und zeitliche Beschränkung, eingeschränkte Verlängerungsmöglichkeit). Im Vergleich mit der Bildübertragung nach Absatz 2 handelt es sich bei den Maßnahmen nach Absatz 3 um eingriffsintensivere Instrumente; die Differenzierung hinsichtlich der Eingriffsschwelle ist daher sachgerecht. Dass die Maßnahmen nach Satz 1 örtlich auf den „erforderlichen Bereich“ zu beschränken und auf sechs Monate zu befristen sind, schränkt die Anwendbarkeit der Maßnahme aus Verhältnismäßigkeitsgründen ein; allerdings bleibt es wegen der tatbestandlichen Fassung der Nrn. 1 – 3 und angesichts der Verlängerungsmöglichkeit bei Fortbestehen der Anordnungsvoraussetzungen bei dem genannten weiten „Einsatzspielraum“ des Instruments.

Absatz 4 erlaubt der Polizei offene Bild- und Tonaufnahmen oder -aufzeichnungen im Zusammenhang mit polizeilichen Maßnahmen zur Eigensicherung. Hinsichtlich des räumlichen Anwendungsbereich wird Gleichlauf mit den vorausgehenden Absätzen hergestellt. Die Regelung ist nicht zu beanstanden und trägt den Eigensicherungsbedürfnissen in angemessener Weise Rechnung.

Eine beachtliche Neuerung stellt die durch Absatz 5 eröffnete Möglichkeit dar, bei den Maßnahmen nach Absatz 1 bis 3 automatisierte Anwendungen zur Datenverarbeitung einzusetzen, die Bewegungsmuster erkennen und auswerten können. Diese Bewegungsmuster müssen auf spezifische Handlungen ausgerichtet sein, mit denen Rechtsgüter von hohem Rang (Leben, Leib, Freiheit oder sexuelle Selbstbestimmung einer Person) gefährdet werden. Damit werden neuere technische Möglichkeiten aufgegriffen, was die Effektivität und „Punktgenauigkeit“ der Videoüberwachung deutlich steigert, zugleich aber grundrechtssensibel und unter Vermeidung von „Racial Profiling“ und ähnlicher diskriminierender Phänomene steuert.

Die Regelung sieht vor, dass bei einem Erkennen solcher Muster durch die automatisierte Anwendung unverzüglich durch qualifizierte Beschäftigte der Polizei geprüft werden muss, ob tatsächlich eine Gefahr für diese Rechtsgüter vorliegt. Hier sollte klargestellt werden, welche „Qualifikation“ die Beschäftigten aufweisen müssen – ausweislich der Begründung des Gesetzentwurfs (S. 41 u.) soll die Anforderung dazu dienen, das Verbot automatisierter Einzelentscheidungen umzusetzen. Welche zusätzliche Regelungswirkung dem Adjektiv „qualifiziert“ zukommen soll, erschließt sich nicht.

Nur bei Vorliegen einer Gefahr und nach Prüfung darf zur Unterstützung gefahrenabwehrender Maßnahmen (eine sachgerechte Zweckbindung) eine automatisierte

Nachverfolgung der verantwortlichen Person durch eine Kennzeichnung in den vorliegenden Bildübertragungen bzw. -aufzeichnungen erfolgen. Zur Kennzeichnung sind „vorrangig“ „nicht körperliche Merkmale“ zu verwenden; auch hier bleibt die normative Relevanz des „vorrangig“ unklar, weil die Formulierung die Verwendung anderer Merkmale nicht ausschließt.

Für den Fall des Einsatzes eines Hochrisiko-KI-Systems verweist die Vorschrift auf verschiedene Pflichten, namentlich die Betreiberpflichten nach Art. 26 der KI-Verordnung. Der Begriff des Hochrisiko-KI-Systems wird dabei zwar nicht im Legaldefinitionen-Katalog des Art. 3 der KI-Verordnung bestimmt, dafür aber durch Art. 6 der KI-Verordnung näher konturiert; es ergibt sich ein gesondertes Regelungsregime, vor allem spezifische Verpflichtungen und Verantwortungen der Betreiber. Soweit in der KI-Verordnung der Terminus „Strafverfolgung“ verwendet wird, beschränkt sich dieser nicht nach dem Verständnis der deutschen Differenzierung zwischen präventiven und repressiven Tätigkeitsfeldern nicht auf letzteren, sondern schließt – wie sich aus Art. 3 Nr. 46 der KI-Verordnung ergibt – auch die Abwehr von Gefahren für die öffentliche Sicherheit ein.

Der Verweis auf die Vorschriften der KI-Verordnung erscheint aufgrund der unmittelbaren Geltung unionsrechtlicher Verordnungen zwar als entbehrlich. Hinzuweisen ist aber darauf, dass sich die Zeitpunkte für das Inkrafttreten der Regelungen der KI-Verordnung zu Hochrisiko-KI-Systeme durch den „Digital Omnibus on AI“ verändert haben. Für Hochrisiko-KI-Systeme für den Bereich der „Strafverfolgung“ gelten die Betreiberpflichten erst ab den 2. Dezember 2027 (Art. 113 S. 3 lit. c) der KI-Verordnung). Damit verweist die Regelung in § 184 Abs. 5 LVwG-E auf eine unionsrechtliche Bestimmung, die selbst erst ab Ende 2027 in Kraft treten wird. Ob damit bei einem früheren Inkrafttreten der Neufassung des LVwG gewissermaßen auch schon die Betreiberpflichten „aktiviert“ werden, ist unklar und sollte jedenfalls klargestellt werden.

Die in Absatz 6 vorgesehenen weiteren Regelungen zur Löschung bzw. Vernichtung und zur Zulässigkeit einer Speicherung erscheinen sachgerecht. Gleiches gilt für Absatz 7, der zum einen die Zulässigkeit der unvermeidbaren Mitbeobachtung Dritter erklärt, zum anderen Hinweispflichten (offene Datenerhebung, Verwendung einer automatisierten Anwendung) regelt.

III. Biometrische Fernidentifizierung

Die biometrische Fernidentifizierung ist eine neuartige, eingriffsintensive Maßnahme, die bislang nur vereinzelt Eingang in die Polizeigesetze gefunden hat. Der Gesetzentwurf sieht sie in zwei Varianten vor: Zum einen als „Echtzeit-Fernidentifizierung“ in öffentlich zugänglichen Räumen (§§ 184b und 184c LVwG-E), zum anderen die nachträgliche Fernidentifizierung (§§ 195b und 195c LVwG-E).

a) Echtzeit-Fernidentifizierung in öffentlich zugänglichen Räumen

Die umfangreichen Vorschriften in §§ 184b, 184c LVwG-E sollen als neu eingefügte Bestimmungen die Echtzeit-Fernidentifizierung im Zusammenhang mit der Videoüberwachung öffentlich zugänglicher Räume regeln. Die § 184b Abs. 1 LVwG-E zugrunde liegende Idee ist, dass die Polizei durch Maßnahmen nach § 184 Abs. 1 oder 3 LVwG-E (Datenerhebung bei öffentlichen Veranstaltungen und Ansammlungen sowie auf und an allgemein zugänglichen Flächen sowie in Räumen und auf befriedetem Besitztum) erlangte Daten in biometrische Daten umwandeln und speichern kann, um sie – als Referenzquellen – „live“ (Echtzeit) mit anderen biometrischen Daten, die die Polizei aus Daten zu Gesichtern oder Stimmen einer Person gewonnen hat, abzugleichen. Dieser Abgleich darf nach den Regelungen des Entwurfs (Absatz 2 S. 2) allein zur Identifizierung einer Person erfolgen. Ziel der Maßnahme muss nach Absatz 1 Satz 1 sein, „vorhandene Sachverhalte“ zu ergänzen.

Nach Absatz 1 Satz 3 ist ein solcher Abgleich nur zulässig, wenn er zur Abwehr einer Gefahr für Leben, Leib, Freiheit oder die sexuelle Selbstbestimmung einer Person bzw. für den Bestand oder die Sicherheit des Bundes oder eines Landes unbedingt erforderlich ist. Damit wird die Maßnahme sachgerecht an anerkanntermaßen besonders gewichtige Rechtsgüter als Eingriffsschwellen angeknüpft. Hintergrund ist die Tatsache, dass bei einer Videoüberwachung typischerweise eine Vielzahl an Daten einer Vielzahl unbeteiligter Personen „mitgehoben“ wird, was die Eingriffsintensität deutlich erhöht und besondere Anforderungen an die Eingriffsschwellen aktiviert. Die tatbestandliche Hürde ist daher angemessen gesetzt.

Normsetzungstechnisch wenig überzeugend erscheint der jeweilige Verweis auf „Ziele“ in Art. 5 UAbs. 1 lit. h) Ziffern i und ii der KI-Verordnung. Die Formulierung „im Hinblick auf die Ziele“ ist nicht hinreichend bestimmt. Soll dies bedeuten, dass die

Maßnahme nur zulässig ist, wenn die in der jeweiligen Norm genannten Ziele verfolgt werden sollen, oder genügt die Gefahr für die aufgeführten Schutzgüter? Bei Nr. 2 werden Schutzgüter gar nicht genannt, so dass es nahe liegt, die Formulierung „im Hinblick auf die Ziele“ im Sinne einer polizeilichen Intention bzw. eines konkreten Zwecks der Maßnahme zu verstehen. Dann sollten aber schlichtweg die in der KI-Verordnung genannten Ziele in bestimmt formulierte Anforderungen umgewandelt werden, etwa

„(...) soweit sie

1. der gezielten Suche nach bestimmten Opfern von Entführung, Menschenhandel oder sexueller Ausbeutung sowie der Suche nach vermissten Personen dient und dabei zur Abwehr einer Gefahr für Leib, Leben, Freiheit oder die sexuelle Selbstbestimmung einer Person unbedingt erforderlich ist oder

2. der Abwehr einer konkreten, erheblichen und unmittelbaren Gefahr für das Leben oder die körperliche Unversehrtheit einer Person dient oder

3. der Abwehr einer tatsächlichen und bestehenden oder tatsächlichen und vorhersehbaren Gefahr eines Terroranschlags dient und dabei zur Abwehr einer Gefahr für Leib, Leben oder Freiheit einer Person oder den Bestand oder die Sicherheit des Bundes oder eines Landes unbedingt erforderlich ist.“

Dass eine „einfache“ konkrete Gefahr gefordert wird, nicht aber etwa eine gegenwärtige, erscheint mit Blick auf die Funktionen der Echtzeit-Fernidentifizierung nachvollziehbar. Dass der Abgleich „unbedingt erforderlich“ sein muss, stellt eine qualifizierte Verhältnismäßigkeitsanforderung dar, die der Normfassung des Art. 5 UAbs. 1 lit. h) der KI-Verordnung entspricht.

Absatz 2 ordnet in Satz 1 (erneut deklaratorisch) an, dass die Maßnahme nach Absatz 1 stets auf das zeitlich und örtlich unbedingt erforderliche Maß zu begrenzen sind. Satz 2 enthält eine klare Zweckbindung hinsichtlich der Identifikation einer natürlichen Person.

Absatz 3 regelt die Antragsbefugnis und einen Richtervorbehalt für Maßnahmen nach Absatz 1. Die weiteren Verfahrensregelungen erscheinen als sachgerecht.

§ 184c LVwG-E trifft Regelungen zur Umsetzung (also: Durchführung) der Echtzeit-Fernidentifizierung. Den verfassungsrechtlichen Vorgaben wird dabei – soweit ersichtlich – Genüge getan. Es finden sich in Absatz 1 Vorgaben zur Verarbeitung und zweckgebundenen Speicherung der biometrischen Daten (die aufgrund der

Weiterverwertbarkeit der Informationen von besonderer verfassungsrechtlicher Relevanz sind), zur Überprüfung des Abgleichsergebnisses durch zwei qualifizierte Beschäftigte der Polizei (zur Sicherstellung des Grundsatzes, dass abschließend ein Mensch auf das Ergebnis schauen soll; zum Problem der „Qualifizierung“ s. o. II.) und zur Löschung. Absatz 2 normiert die Unterrichtung des Betroffenen. In Absatz 3 finden sich Bestimmungen zum Kreis der Zugangsberechtigten und ergänzende Vorschriften einschließlich einer Ermächtigung zur Regelung von Einzelheiten in einer Verwaltungsvorschrift.

b) Nachträgliche Fernidentifizierung

Der Entwurf schlägt die Aufnahme der neuen Bestimmungen in §§ 195b und 195c LVwG-E zur nachträglichen Fernidentifizierung vor. Die Vorschriften ähneln teilweise denjenigen zur Echtzeit-Fernidentifizierung, so dass auf die Ausführungen oben unter a) verwiesen werden kann. Die Eingriffsschwellen in § 195b Abs. 1 LVwG-E erscheinen als verfassungskonform festgesetzt. Zu begrüßen ist die Anknüpfung an die Rechtsgüter Leben, Leib, Freiheit bzw. sexuelle Selbstbestimmung einer Person sowie den Bestand oder die Sicherheit des Bundes oder eines Landes. Auch das Verbot, biometrische Daten aus im Internet in Echtzeit übertragenen und veröffentlichten Video-, Audio- oder Bilddateien zu gewinnen und für die Fernidentifikation zu nutzen, stellt eine sinnvolle Einschränkung dar. Zur Kritik an der Formulierung „zur Ergänzung eines vorhandenen Sachverhalts“ s. u. IV.

Die weiteren Bestimmungen in § 195b LVwG-E und die Durchführungsbestimmungen in § 195c LVwG-E erscheinen sachgerecht.

IV. IT-gestützter Abgleich, Datenanalyse

§ 188c LVwG-E sieht die Möglichkeiten eines IT-gestützten (Daten-)Abgleichs und der Datenanalyse vor. § 188d LVwG-E enthält Durchführungsbestimmungen. Regelungssystematisch ist diese getrennte normative Festsetzung (Voraussetzungen, Verfahrensregelungen) sinnvoll, um die Normen nicht zu unübersichtlich werden zu lassen.

Im Übrigen sind beide Vorschriften komplex und umfangreich; die wesentlichen verfassungsrechtlichen Anforderungen an den IT-gestützten Abgleich als weniger belastendes, die Datenanalyse als eingriffsintensiveres Instrument sind nach Einschätzung des

Unterzeichners aber berücksichtigt, und die differenzierten Vorgaben des Bundesverfassungsgerichts erscheinen als in gut vertretbarer Weise umgesetzt. Im Detail sind Optimierungen möglich. Ansonsten ist die Aufnahme der Maßnahmen in den LVwG-E aber mit Blick auf eine technikoffene, moderne Polizeiarbeit uneingeschränkt überzeugend.

§ 188c Abs. 1 S. 1 LVwG-E erlaubt die zweckgebundene Zusammenführung von personenbezogenen Daten für die Dauer der Bearbeitung vorhandener Sachverhalte, um anhand zielgerichteter Suchkriterien Übereinstimmungen zwischen diesen Daten festzustellen (IT-gestützter Abgleich).

Diese Formulierung – „vorhandene Sachverhalt“ – erscheint aber als sprachlich nicht geschickt und letztlich polizeirechtlich systemfremd – Sachverhalte können nicht „vorhanden“ sein, sondern z. B. bekannt oder „ausermittelt“; vorhanden sind vielmehr personenbezogene Informationen, aus deren Gesamtschau sich dann ein Sachverhalt ergibt. Der Norm geht es um die Vervollständigung eines tatsächlichen Lagebildes bzw. Tatkomplexes durch Ergänzung bereits bei der Polizei vorliegender Informationen. Der Begriff des „vorhandenen Sachverhalts“ ist im Polizeirecht ungebräuchlich. Die Intention des Entwurfs, die fraglichen Maßnahmen auf den Kontext eines bestimmten polizeilichen Tatsachenkomplex zu beziehen und damit auch gewissermaßen hinsichtlich der Zielsetzung einzuhegen, ist erkennbar; gleichwohl handelt es sich um eine polizeirechtsfremde Kategorie. Es bietet sich daher an, den Passus in den betroffenen Normen „zur Ergänzung vorhandener personenbezogener Daten“ umzuformulieren.

Wenig überzeugend ist es zudem, wenn § 188c Abs. 1 S. 1 LVwG-E (wie auch Absatz 2 Satz 1) an die Voraussetzungen des § 188a Abs. 1 und 2 LVwG, des § 479 Abs. 2 S. 2 Nr. 1 und 2 StPO andererseits anknüpft. Die Formulierung (auch in Absatz 2) „nach Maßgabe“ wird in dem Sinne verstanden werden müssen, dass die tatbestandlichen Voraussetzungen der genannten Bestimmungen erfüllt sein müssen.

Absatz 2 erlaubt es der Polizei, in polizeilichen Datensystemen gespeicherte personenbezogene Daten mittels einer automatisierten Anwendung zur Datenverarbeitung zu den in Absatz 3 und 4 beschriebenen Zwecken anlassbezogen zusammenführen und anschließend zur Gewinnung neuer Erkenntnisse verarbeiten. Damit erlaubt Absatz 1 den IT-gestützten Abgleich, Absatz 2 die (automatisierte) Datenanalyse. Die gewählten Eingriffsschwellen, die den Verweisonormen zu entnehmen sind (zur Kritik s. o.), erscheinen hinsichtlich dieser beiden Instrumente verfassungsrechtlich zulässig.

Die eigentlichen Voraussetzungen für eine eingeschränkte Form der Datenanalyse regelt Absatz 3: Hier geht es um eine Datenanalyse, die nur bestimmte Quellen nutzt, namentlich personenbezogene Daten aus Vorgangs- und Fallbearbeitungssystemen, polizeilichen Auskunfts-, Kommunikations-, Einsatzleit- und Einsatzdokumentationssystemen sowie Asservaten. Die Eingriffsschwellen und die Regelungen zu den geschützten Rechtsgütern sind dabei nicht zu beanstanden. Was mit „anderen Beweismitteln“ gemeint sein soll, erschließt sich nicht; die Formulierung erscheint angesichts der unmittelbar vorausgehenden klaren Aufzählung der zulässigen Quellen als zu unbestimmt.

Eine hinsichtlich der Quellen weiter gefasste Form der Datenanalyse ermöglicht Absatz 4. Wenn und soweit personenbezogene Daten aus sämtlichen Datensystemen der Polizei und automatisierten Verfahren einbezogen werden sollen, kann dies nur zur Abwehr einer Gefahr für Leben, Leib, Freiheit oder die sexuelle Selbstbestimmung einer Person, den Bestand oder die Sicherheit des Bundes oder eines Landes erfolgen (Satz 1 mit Verweis auf Absatz 3 S. 2 Nr. 1). Der vom Bundesverfassungsgericht in mehreren Entscheidungen formulierten Anforderung, dass jeweils auch zu berücksichtigen ist, mittels welcher Maßnahme die fraglichen Daten gewonnen wurden, trägt Satz 2 Rechnung, indem für den Fall der Verarbeitung personenbezogener Daten, die durch den Einsatz technischer Mittel in Wohnungen erhoben wurden, die Eingriffsschwelle auf eine dringende Gefahr angehoben wird. Diese Gefahrenkategorie ist Art. 13 GG entnommen, wobei es sich angesichts der nach wie vor bestehenden begrifflichen Unklarheiten anbieten würde, die gefährdeten Rechtsgüter zu ergänzen. So spricht beispielsweise § 185 Abs. 3 S. 1 LVwG (besondere Mittel der Datenerhebung) von einer „dringenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person“. Dies könnte auch in Absatz 4 Satz 2 ergänzt werden.

Die weiteren Regelungen in § 188c LVwG-E sowie diejenigen des § 188d LVwG-E begegnen keinen (verfassungs-)rechtlichen Bedenken; wie auch in den anderen Vorschriften zur Umsetzung bzw. Durchführung einzelner Maßnahmen sind heterogene verfassungsrechtliche Anforderungen vorgesehen.

V. Elektronische Aufenthaltsüberwachung

Regelungen zu einer elektronischen Aufenthaltsüberwachung finden sich mittlerweile in zahlreichen Landespolizeigesetzen. § 201b LVwG-E sieht eine umfassende Neuregelung vor, die insgesamt zu begrüßen ist.

Herausgegriffen kann etwa die an das Konzept der „spanischen Fußfessel“ angelehnte Regelung in Absatz 3: Sie sieht vor, dass auch eine individualisierbare gefährdete Person freiwillig ein technisches Mittel mit sich führt, über das die Polizei Daten über ihren Aufenthaltsort automatisiert erheben, speichern und mit dem Aufenthaltsort der überwachten Person abgleichen. Dies ist sachgerecht, weil die Anordnung einer elektronischen Aufenthaltsüberwachung kein „Selbstzweck“ zur umfassenden Datenerhebung hinsichtlich der überwachten Person ist, sondern immer aufenthaltsbestimmende Anordnungen flankieren und ihre Einhaltung kontrollieren soll. Dabei geht es sich allein um statische „Verbotzonen“. Angesichts der Schutzziele der Maßnahme ist es praktikabel, Kontakt- und Näherungsverbote bezüglich einer „mobilen“ gefährdeten Person durch zwei technische Geräte zu überwachen.

§ 201c LVwG-E soll eine Befugnisnorm für die elektronische Aufenthaltsüberwachung bei terroristischen Gefahren schaffen. Die normierten Voraussetzungen sind an die Rechtsprechung des Bundesverfassungsgerichts zur „hinreichend konkretisierten Gefahr“ angelehnt; dies ist nicht zu beanstanden, auch weil als zusätzliche Anforderung verlangt wird, dass die Überwachung des Aufenthaltsortes der betroffenen Person unerlässlich ist, um die befürchtete terroristische Straftat zu verhindern. Dass die Norm zugleich eine „Legaldefinition“ der terroristischen Straftat enthält, ist zu begrüßen. Es handelt sich um gängige Formulierungen. Dies gilt auch für die weiteren Absätze der Norm und für § 201d LVwG-E zur Anordnung der elektronischen Aufenthaltsüberwachung.

VI. Gewahrsam

Die vorgesehenen Anpassungen in den gesetzlichen Bestimmungen zum Gewahrsam sind zu begrüßen. Sie entsprechen durchweg den Anforderungen im Zusammenhang mit derart eingriffsintensiven Maßnahmen.

In § 204 Abs. 1 Nr. 2 LVwG-E sind vor allem Konkretisierungen zum Präventivgewahrsam vorgesehen. Wie bisher wird auf die Annahme einer Begehung oder Fortsetzung einer Tat abgestellt. Der Normvorschlag nimmt allerdings bestimmte konkrete Fallgruppen

(„insbesondere“) auf und beschreibt Tatsachen, auf die sich diese Annahme stützen kann. Die Aufzählung ist nicht abschließend, typisiert aber in überzeugender Weise Sachverhaltskonstellationen, in denen ein Präventivgewahrsam in Betracht kommen kann, aber nicht muss. Die Fallgruppen (Tatbekenntnis, Auffinden bestimmter Gegenstände, Wiederholungsgefahr) sind als „legislative Prognosehilfen“ überzeugend formuliert. Da sie die Bewertung lediglich unterstützen, nicht aber maßgeblich lenken sollen, handelt es sich normtechnisch nicht um „Regelbeispiele“ für eine der tatbestandlichen Anforderungen. Es könnte sich daher anbieten, von der Verwendung des Wortes „insbesondere“ abzusehen, das häufig die Normierung von Regelbeispielen signalisiert, bei deren Vorliegen nach gesetzgeberischer Vorwertung auch das Tatbestandsmerkmal gegeben sein soll.

Ein Einwand lässt sich gegen die Prognosehilfen allerdings vorbringen: In § 204 Abs. 1 Nr. 2 lit. b) LVwG-E wird auf Begleitpersonen abgestellt, die bestimmte Gegenstände mit sich führen und von denen die in Gewahrsam genommene Person den Umständen nach Kenntnis haben musste. Unklar bleibt, was unter „Begleitperson“ zu verstehen ist. Der Begriff wird im LVwG auch an vereinzelt anderen Stellen verwendet, ohne dass klar würde, welche Personen er erfassen soll. Die Begründung führt dazu Näheres aus und knüpft an den Eindruck einer Zusammengehörigkeit an (S. 71), angesichts der Bedeutung des Begriffs sollte aber eine Legaldefinition erfolgen. Entsprechende Begriffsbestimmungen in anderen Polizeigesetzen (z. B. § 16a Abs. 1 S. 4 PolG NRW) lassen sich dabei nur sehr eingeschränkt nutzen, weil häufig eine Abgrenzung zu den Kontaktpersonen vorgenommen wird.

Dass mit § 204 Abs. 1 Nr. 3 LVwG-E ein neuer Gewahrsamstatbestand geschaffen werden soll, der nicht an die Begehung oder Fortsetzung von Ordnungswidrigkeiten von erheblicher Bedeutung für die Allgemeinheit oder von Straftaten anknüpft, sondern an gefährdete Rechtsgüter von besonderem Gewicht, ist ohne weiteres zu befürworten. Sicherlich wird bei einer Gefahr für diese Rechtsgüter regelmäßig zwar auch eine bevorstehende Straftat in Rede stehen; Nr. 2 erfordert aber eine unmittelbar bevorstehende Begehung bzw. Fortsetzung der Tat; die Abwehr einer Gefahr verlagert den zeitlichen Ansatzpunkt für die Ingewahrsamnahme deshalb nach vorn, weil nach gängiger polizeirechtlicher Dogmatik die Anforderungen an die Bejahung der hinreichenden Wahrscheinlichkeit eines Schadenseintritts bei besonders gewichtigen Rechtsgüter niedriger sind als bei weniger bedeutenden (sog. „je-desto“-Formel). Dass damit die Ingewahrsamnahme als Maßnahme von gravierender Eingriffsintensität bei Nr. 3 schon „früher“ zulässig sein kann

als nach Nr. 2, ist verfassungsrechtlich aufgrund der Anbindung an den gewählten Rechtsgüterkatalog nicht zu beanstanden.

§ 205 und § 205a LVwG-E ordnen die Vorschriften für die Behandlung von in Gewahrsam genommenen Personen sowie die richterliche Entscheidung neu. Wesentliche verfassungsrechtliche Vorgaben werden aufgenommen. Beispielfhaft genannt werden kann die Bestellung einer anwaltlichen Vertretung (§ 205a Abs. 3 LVwG-E), wobei (wie übrigens auch in anderen Landesgesetzen) unklar bleibt, ob sich der Vergütungsanspruch (bezüglich dessen in § 205a Abs. 5 S. 2 LVwG-E auf das Rechtsanwaltsvergütungsgesetz verwiesen wird) gegen die in Gewahrsam genommene Person als Nutznießer der Vertretung oder aber gegen den von Amts wegen bestellenden Staat richtet.

Die weiteren vorgeschlagenen Bestimmungen des Gesetzentwurfs entsprechen nach Einschätzung des Unterzeichners den verfassungsrechtlichen Vorgaben bzw. sind jedenfalls gut vertretbare Regelungsvarianten.

VII. Kontrollen in den Küstengewässern

Die im Änderungsantrag vorgeschlagene neue Vorschrift in § 181b LVwG-E/Ä sieht eine Befugnis zum Anhalten, Betreten und Inaugenscheinnahmen von Wasserfahrzeugen im Küstenmeer und in den landeinwärts zur Basislinie des Küstenmeeres gelegenen Gewässern vor. Auch eine Identitätsfeststellung von an Bord befindlichen Personen soll ermöglicht werden. Satz 2 enthält eine verfassungsrechtliche gebotene Einschränkung für die Ausübung dieser Befugnisse außerhalb der „Betriebs- und Geschäftszeiten“; dies trägt der Tatsache Rechnung, dass auch Wasserfahrzeuge als „Wohnung“ im Sinne des Art. 13 GG dienen können. Die Beschränkung auf eine „Inaugenscheinnahme“ soll neben dem Betreten ein „Sichumsehen“ ermöglichen, das aber die Schwelle zur einer Durchsuchung nicht überschreiten darf. Insgesamt erscheint die vorgeschlagene Vorschrift als sinnvoll und sachgerecht ausgestaltet.

VIII. Automatisierte Datenerhebung im öffentlichen Verkehrsraum zur Erkennung von Ablenkungsverstößen

Der im Änderungsentwurf vorgeschlagene neue § 184d LVwG-E/Ä soll im öffentlichen Verkehrsraum durch den offenen Einsatz automatisierter Anwendungen zur

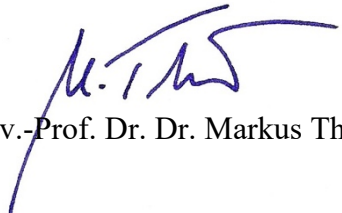
Bildübertragung und Bildaufzeichnung stichprobenweise personenbezogene Daten erheben und verarbeiten dürfen. Dies soll dazu dienen, die unerlaubte Benutzung von elektronischen Geräten i.S.v. § 23 Abs. 1a StVO zu „verhüten“. Diese Regelung mag aus praktischer Sicht sachgerecht erscheinen; sie ist aber doch sehr spezifisch allein auf einen sanktionierten Normverstoß der StVO ausgerichtet. Es geht – wie sich auch aus der eher „nachrangigen“ Stellung des Absatz 2 zur Ahndung tatsächlicher Verstöße ergibt – damit in erster Linie um eine „Abschreckung“ durch offen erkennbare Überwachungsmaßnahmen. Der konkrete Verstoß gegen die StVO-Norm wird auch nur an derjenigen Stelle „verhindert“, an der sich erkennbar ein Erfassungsgerät befindet.

Vor diesem Hintergrund hat der Unterzeichner erhebliche Bedenken, ob eine derartige automatisierte Datenerhebung, die ja gerade nicht in erster Linie der Datenerhebung dienen soll, von der polizeilichen Aufgabe der Straftatenverhütung erfasst wird. Es sollte auf die Schaffung dieser Vorschrift verzichtet werden.

IX. Maßnahmen gegen unbemannte Fahrzeugsysteme

§ 213a LVwG-E/Ä sieht eine Befugnisnorm für Maßnahmen gegen unbemannte Fahrzeugsysteme vor. Dem korrespondiert § 185d LVwG-E/A über die Datenerhebung zur Abwehr unbemannter Fahrzeugsysteme. Der Unterzeichner vertritt die Auffassung, dass den Landesgesetzgebern für solche Bestimmungen eine Legislativkompetenz nicht zusteht. Die Begründung des Änderungsantrags setzt sich mit dieser Auffassung kritisch auseinander. Der Unterzeichner hält auch vor diesem Hintergrund an seiner Einschätzung fest; angesichts der Regelungspraxis in zahlreichen anderen Ländern kann das Risiko der Schaffung möglicherweise kompetenzwidriger Normen wohl eingegangen werden.

Münster, den 11. September 2026


(Univ.-Prof. Dr. Dr. Markus Thiel)