Schleswig-Holsteinischer Landtag
Umdruck 20/6786

An den Vorsitzenden des Innen- und Rechtsausschusses

6. Juli 2026

Vorlage für den Innen- und Rechtsausschuss

Änderungsantrag

der Fraktionen von CDU und BÜNDNIS 90/DIE GRÜNEN

zu Drucksache 20/4284

Der Landtag wolle beschließen:

Artikel 1 (Änderung des Landesverwaltungsgesetzes) wird wie folgt geändert:

1. Nummer 1 wird wie folgt gefasst:

‚**1. Die Inhaltsübersicht wird wie folgt geändert:**

a) Nach der Angabe zu § 181a wird folgende Angabe eingefügt:

„§ 181b Kontrollen in den Küstengewässern zum Schutz von Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen“

b) Die Angabe zu § 184 erhält folgende Fassung:

„§ 184 Datenerhebung bei öffentlichen Veranstaltungen und Ansammlungen sowie an allgemein zugänglichen Orten“

c) Nach der Angabe zu § 184a werden folgende Angaben eingefügt:

„§ 184b Echtzeit-Fernidentifizierung in öffentlich zugänglichen Räumen“

„§ 184c Durchführung der Echtzeit-Fernidentifizierung in öffentlich zugänglichen Räumen“

„§ 184d Automatisierte Datenerhebung im öffentlichen Verkehrsraum zur Erkennung von Ablenkungsverstößen“

d) Die Angabe zu § 185a erhält folgende Fassung:

„§ 185a Überwachung der Telekommunikation und Erhebung von Verkehrsdaten“

e) Nach der Angabe zu § 185c werden folgende Angaben eingefügt:

„§ 185d Datenerhebung zur Abwehr unbemannter Fahrzeugsysteme“

„§ 185e Datenerhebungen mittels mobiler Sensorträgersysteme“

f) Die Angabe zu § 186a erhält folgende Fassung:

„§ 186a Grundsätze der Datenverarbeitung bei Maßnahmen nach §§ 185, 185a und § 185c“

g) Nach der Angabe zu § 188b werden folgende Angaben eingefügt:

„§ 188c IT-gestützter Abgleich; Datenanalyse“

„§ 188d Durchführung des IT-gestützten Abgleichs und der Datenanalyse“

h) Nach der Angabe zu § 195a werden folgende Angaben eingefügt:

„§ 195b Nachträgliche Fernidentifizierung“

„§ 195c Durchführung der nachträglichen Fernidentifizierung“

i) Die Angabe zu § 201b erhält folgende Fassung:

„§ 201b Elektronische Aufenthaltsüberwachung bei Gefahren für wichtige Rechtsgüter“

j) Die Angabe zu § 201c erhält folgende Fassung:

„§ 201c Elektronische Aufenthaltsüberwachung bei terroristischen Gefahren“

k) Nach der Angabe zu § 201c wird folgende Angabe eingefügt:

„§ 201d Anordnung der elektronischen Aufenthaltsüberwachung“

l) Die Angabe zu § 205 erhält folgende Fassung:

„§ 205 Behandlung in Gewahrsam genommener Personen“

m) Nach der Angabe zu § 205 wird folgende Angabe eingefügt:

„§ 205a Richterliche Entscheidung bei Gewahrsam; rechtsanwaltliche Vertretung“

n) Nach der Angabe zu § 213 wird folgende Angabe eingefügt:

„§ 213a Maßnahmen gegen unbemannte Fahrzeugsysteme“ ‘

2. Nach Nummer 1 werden folgende Nummern 2 und 3 eingefügt:

‚**2. In § 179 werden nach Absatz 5 folgende Absätze 6 und 7 eingefügt:**

„(6) Die Polizei kann die bei der Herstellung einer Notrufverbindung zu einer polizeilichen Notrufeinrichtung anfallenden Standortdaten ohne Wissen der betroffenen Person automatisiert erheben und speichern sowie, wenn dies zur Abwehr einer Gefahr erforderlich ist, weiterverarbeiten. Absatz 5 Satz 2 gilt entsprechend. Maßnahmen nach § 185a bleiben unberührt.

(7) Um eine geeignete Notrufkommunikation von Menschen mit Behinderungen zu gewährleisten, kann das für Inneres zuständige Ministerium durch Rechtsverordnung Regelungen für die Annahme und Beantwortung von Notrufen über die Notrufnummer 110 treffen, insbesondere zur Form der Annahme und zur Zeit bis zur Annahme.“

3. § 180a Absatz 4 wird wie folgt gefasst:

„(4) Absatz 1 bis 3 gelten bei an geschäftsmäßig handelnde Anbieter von digitalen Diensten gerichteten Auskunftsverlangen auf Bestandsdaten nach § 2 Absatz 2 Nummer 2 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982, ber. 2022 I S. 1045), zuletzt geändert durch Artikel 3 des Gesetzes vom 10. März 2026 (BGBl. 2026 I Nr. 64) sowie auf die Identifikation der Nutzer und auf das Datum und die Uhrzeit des Beginns und Endes der Verarbeitung beschränkte Daten im Sinne des § 2 Ab-

satz 2 Nummer 3 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes entsprechend, soweit dies zur Abwehr einer im einzelnen Falle bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person sowie zur Abwehr einer gegenwärtigen Gefahr eines gleichgewichtigen Schadens für Sach- oder Vermögenswerte oder für die Umwelt erforderlich ist. Auskunftsverlangen nach Satz 1, die auf als Bestandsdaten erhobene Passwörter oder andere Daten gerichtet sind, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird, sind nur zur Abwehr einer konkreten Gefahr für Leib, Leben oder Freiheit einer Person zulässig. Das vom Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz zum Inhalt und zur Übermittlung des Auskunftsverlangens an geschäftsmäßig handelnde Anbieter von digitalen Diensten vorgegebene Verfahren gemäß § 22 Absatz 2 und § 24 Absatz 2 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes findet Anwendung.“ ‘

3. Die bisherige Nummer 2 wird zur Nummer 4.

4. Nach dem Änderungsbefehl zu § 181 (neue Nummer 4) werden folgende Nummern 5 und 6 eingefügt:

‚**5. Nach § 181a wird folgender § 181b eingefügt:**

„**§ 181b**

Kontrollen in den Küstengewässern zum Schutz von Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen

Soweit es aufgrund bestimmter Tatsachen zur Abwehr einer Gefahr für wesentliche Infrastruktureinrichtungen oder Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen erforderlich erscheint, darf die Polizei im Küstenmeer und in den landeinwärts zur Basislinie des Küstenmeeres gelegenen inneren Gewässern gemäß Artikel 8 Seerechtsübereinkommen der Vereinten Nationen (BGBl. II 1994 S. 1799)

1. ein Wasserfahrzeug, einschließlich der Betriebs- und Geschäftsräume, betreten und in Augenschein nehmen und,

2. soweit dies für Maßnahmen nach Nummer 1 erforderlich ist, das Wasserfahrzeug anhalten, sowie

3. die Identität von Personen feststellen, die sich auf dem Wasserfahrzeug befinden.

Außerhalb der Betriebs- und Geschäftszeiten und hinsichtlich der Räume, die zugleich Wohnzwecken dienen, dürfen diese Befugnisse nur zur Verhütung dringender Gefahren für die öffentliche Sicherheit ausgeübt werden. Die schifffahrtspolizeilichen Aufgaben der Polizei bleiben unberührt.“ ‘

6. § 183 wird wie folgt geändert:

a) Absatz 1 Satz 3 wird wie folgt gefasst:

„Darüber hinaus dürfen Polizeivollzugsbeamtinnen und Polizeivollzugsbeamte die zur Verhütung einer künftigen Straftat erforderlich erscheinenden erkennungsdienstlichen Maßnahmen anordnen, wenn die betroffene Person dringend verdächtig ist, eine mit Strafe bedrohte Handlung im Sinne des § 179 Absatz 2 begangen zu haben, und wenn Tatsachen, insbesondere die Art, Ausführung oder Schwere der Tat sowie die Persönlichkeit der tatverdächtigen Person, die Annahme rechtfertigen, dass die Person zukünftig gleichartige Straftaten begehen wird.“

b) Nach Absatz 2 wird folgender Absatz 2a eingefügt:

„(2a) Unter den Voraussetzungen des Absatzes 1 Satz 1 dürfen Polizeivollzugsbeamtinnen und Polizeivollzugsbeamte auch mit den durch die erkennungsdienstliche Behandlung erhobenen Daten im Sinne des Absatzes 2 einen Abgleich gemäß § 195 durchführen. Soweit erforderlich dürfen sie zu demselben Zweck ergänzend den gemeinsamen Speicher für Identitätsdaten nach Maßgabe des jeweiligen Artikels 20 der Verordnung (EU) 2019/817[1] und der Verordnung (EU) 2019/818[2] abfragen. Der Abgleich, die Abfrage und die hierfür erforderliche Verarbeitung personenbezogener Daten, insbesondere biometrischer Daten, sind nur zulässig, wenn und soweit sie zur Identifizierung der betroffenen Person zwingend erforderlich sind. Die durch die Abfrage er-

[1] Verordnung (EU) 2019/817 des Europäischen Parlaments und des Rates vom 20. Mai 2019 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenzen und Visa und zur Änderung der Verordnungen (EG) 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 und (EU) 2018/1861 des Europäischen Parlaments und des Rates, der Entscheidung 2004/512/EG des Rates und des Beschlusses 2008/633/JI des Rates (ABl. L 135 S. 27; ber. 2020 ABl. L 10 S. 4).
[2] Verordnung (EU) 2019/818 des Europäischen Parlaments und des Rates vom 20. Mai 2019 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen (polizeiliche und justizielle Zusammenarbeit, Asyl und Migration) und zur Änderung der Verordnungen (EU) 2018/1726, (EU) 2018/1862 und (EU) 2019/816 (ABl. L 135 S. 85).

langten personenbezogenen Daten dürfen ausschließlich zur Identifizierung der betroffenen Person verarbeitet werden.“

c) In Absatz 3 werden nach den Wörtern „zu vernichten“ die Wörter „und Daten zu löschen“ eingefügt.‘

5. Die bisherigen Nummer 3 wird zur Nummer 7.

6. Nummer 4 wird wie folgt geändert:

a) Nummer 4 wird zu Nummer 8

b) Der Änderungsbefehl wird wie folgt gefasst:

‚**8. Nach § 184a werden folgende §§ 184b, 184c und § 184d eingefügt:‘**

c) Nach § 184c wird folgender § 184d eingefügt:

„**§ 184d**

Automatisierte Datenerhebung im öffentlichen Verkehrsraum zur Erkennung von Ablenkungsverstößen

(1) Die Polizei darf zur Verhütung der unerlaubten Benutzung von elektronischen Geräten im Sinne des § 23 Absatz 1a der Straßenverkehrs-Ordnung vom 6. März 2013 (BGBl. I S. 367), zuletzt geändert durch Artikel 4 der Verordnung vom 30. Januar 2026 (BGBl. 2026 I Nr. 32) im öffentlichen Verkehrsraum durch den offenen Einsatz automatisierter Anwendungen zur Bildübertragung und Bildaufzeichnung stichprobenweise personenbezogene Daten in dem in Satz 2 beschriebenen Umfang erheben und verarbeiten. Zur Durchführung der Maßnahme darf die Polizei

1. Bildaufzeichnungen von Fahrzeugen und Fahrzeugführenden anfertigen und das Kennzeichen des Fahrzeuges erfassen,

2. Ort, Zeit der Bildaufzeichnung und die Fahrtrichtung Fahrzeugs dokumentieren und

3. die Bildaufzeichnungen von Fahrzeugführenden mit Hilfe bildverarbeitender Systeme auf Muster hin automatisiert auswerten, die auf die unerlaubte Benutzung von elektronischen Geräten im Sinne von Satz 1 hindeuten.

Eine über eine Stichprobe hinausgehende Datenerhebung und Datenverarbeitung in Sinne von Satz 1 und 2 ist nur zulässig, wenn dies aufgrund dokumentierter polizeilicher Lageerkenntnisse erforderlich erscheint. Eine Datenerhebung nach dieser Vorschrift darf auch erfolgen, wenn Dritte unvermeidbar betroffen werden.

(2) Deutet die automatisierte Auswertung der Bildaufzeichnungen auf die unerlaubte Benutzung eines elektronischen Geräts hin, ist die Bildaufzeichnung unverzüglich durch entsprechend qualifizierte Beschäftige der Polizei auf einen Verstoß gegen § 23 Absatz 1a der Straßenverkehrs-Ordnung hin zu überprüfen. Erst nach einer Bestätigung des Verstoßes ist die weitere Verarbeitung der gemäß Absatz 1 erhobenen Daten nach dieser oder anderen Vorschriften zulässig. Bis zur Bestätigung des Verstoßes darf das Fahrzeug angehalten werden.

(3) Deutet die automatisierte Auswertung der Bildaufzeichnungen nicht auf die unerlaubte Benutzung eines elektronischen Geräts hin oder wird ein Verstoß gegen § 23 Absatz 1a der Straßenverkehrs-Ordnung nicht bestätigt, sind alle gemäß Absatz 1 erhobenen Daten sofort, spurenlos und automatisiert zu löschen.

(4) Die Datenerhebung und Datenverarbeitung ist nach Maßgabe von § 186c zu protokollieren, soweit die automatisierte Auswertung der Bildaufzeichnungen auf die unerlaubte Benutzung eines elektronischen Geräts hindeutet. Im Übrigen ist eine Protokollierung unzulässig; es ist jedoch ein technisches Systemprotokoll ohne Personen- oder Kennzeichenbezug, insbesondere über Zeitpunkte und Verarbeitungsvorgänge einschließlich der Löschungen, zu erstellen. Die oder der Landesbeauftragte für Datenschutz führt Überprüfungen der Datenverarbeitung bezüglich Maßnahmen gemäß dieser Vorschrift nach Maßgabe von § 186b Absatz 1 durch.

(5) Maßnahmen nach Absatz 1 sind schriftlich anzuordnen, wobei Umfang und Dauer der Datenerhebung sowie die für die Auswahl der Stichprobe wesentlichen Gesichtspunkte und in Fällen des Absatz 1 Satz 2 die zugrundeliegenden Lageerkenntnisse anzugeben sind. Wird für eine Maßnahme nach dieser Vorschrift ein Hochrisiko-KI-System im Sinne der Verordnung (EU) 2024/1689 verwendet, muss die Polizei die Betreiberpflichten nach Artikel 26 Absatz 1 bis 6 sowie Absatz 9 und 12 der Verordnung (EU) 2024/1689 erfüllen. Im Falle des Satzes 2 gelten für die Unterrichtungspflicht nach Artikel 26 Absatz 11 der Verordnung (EU) 2024/1689 die Vorschriften des § 186 Absatz 7 und 8 entsprechend.“

7. Nach dem Änderungsbefehl zur Einfügung von § 184b und weiterer Vorschriften (neue Nummer 8) werden folgende Nummern 9 bis 15 eingefügt:

,**9. § 185 wird wie folgt geändert:**

a) Absatz 2 wird wie folgt gefasst:

„(2) Mit den in Absatz 1 genannten Mitteln darf die Polizei personenbezogene Daten erheben, wenn

1. eine gegenwärtige erhebliche Gefahr abzuwehren ist oder

2. wenn bestimmte Tatsachen die Annahme rechtfertigen, dass ein besonders gewichtiges Rechtsgut im Sinne des Satz 2 innerhalb eines absehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierten Weise durch einen Angriff von erheblicher Intensität oder Auswirkung gefährdet wird,

und die Maßnahme zur Aufklärung des Sachverhalts unerlässlich ist. Besonders gewichtige Rechtsgüter sind Leben, Leib, Freiheit oder die sexuelle Selbstbestimmung einer Person sowie Bestand oder Sicherheit des Bundes oder eines Landes und wesentliche Infrastruktureinrichtungen oder Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen.“

b) In Absatz 3 wird der zweite Satz gestrichen.

10. § 185a wird wie folgt gefasst:

„§ 185a

Überwachung der Telekommunikation und Erhebung von Verkehrsdaten

(1) Die Polizei darf ohne Wissen der betroffenen Person personenbezogene Daten durch Überwachung und Aufzeichnung der Telekommunikation nur erheben zur Abwehr einer dringenden Gefahr für besonders gewichtige Rechtsgüter gemäß § 185 Absatz 2 Satz 2, wenn dieses zur Aufklärung des Sachverhalts unerlässlich ist. Eine Maßnahme im Sinne von Satz 1 ist auch zulässig, wenn das individuelle Verhalten der betroffenen Person eine konkrete Wahrscheinlichkeit dafür begründet, dass sie innerhalb eines übersehbaren Zeitraums eine terroristische Straftat im Sinne des Satzes 3 begehen wird, und die Datenerhebung unerlässlich ist, um die Straftat zu verhindern. Eine terroristische Straftat ist eine der in § 129a Absatz 1 oder Absatz 2 Nummer 1 bis 3 des Strafgesetzbuchs bezeichneten Straftaten, deren Versuch oder Begehung dazu bestimmt ist,

1. die Bevölkerung auf erhebliche Weise einzuschüchtern,

2. eine Behörde oder eine internationale Organisation rechtswidrig mit Gewalt oder durch Drohung mit Gewalt zu nötigen oder

3. die politischen, verfassungsrechtlichen, wirtschaftlichen oder sozialen Grundstrukturen eines Staates oder einer internationalen Organisation zu beseitigen oder erheblich zu beeinträchtigen,

und die durch die Art ihrer Begehung oder ihre Auswirkungen das Land Schleswig-Holstein, die Bundesrepublik Deutschland, ein anderes Bundesland, einen anderen Staat oder eine internationale Organisation erheblich schädigen kann.

(2) Eine Datenerhebung nach Absatz 1 kann sich beziehen auf

1. die Inhalte der Telekommunikation einschließlich der innerhalb des Telekommunikationsnetzes in Datenspeichern abgelegten Inhalte,

2. Verkehrsdaten gemäß § 3 Nummer 70 des Telekommunikationsgesetzes vom 23. Juni 2021 (BGBl. I S. 1858), zuletzt geändert durch Artikel 2 des Gesetzes vom 12. Mai 2026 (BGBl. 2026 I Nr. 138) einschließlich gespeicherter Standortdaten in Sinne von § 3 Nummer 56 des Telekommunikationsgesetzes, soweit diese als Verkehrsdaten angefallen sind,

3. den Standort eines aktiv geschalteten Mobilfunkendgeräts oder

4. die Feststellung der Polizei nicht bekannter Telekommunikationsanschlüsse (Gerätenummer eines Mobilfunkendgerätes und die Kartennummer der darin verwendeten Karte).

Datenerhebungen dürfen sich in den Fällen der Nummer 2 bis 4 auch auf zurückliegende Zeiträume erstrecken; eine Abfrage von Daten, die aufgrund einer gesetzlichen Verpflichtung durch Anbieter von Telekommunikationsdiensten für bestimmte Zeiträume gespeichert werden müssen, ist nicht zulässig.

(3) Eine Datenerhebung nach Absatz 1,

1. mit der Standortdaten erhoben werden oder

2. alle in einer Funkzelle angefallenen Verkehrsdaten abgefragt werden (Funkzellenabfrage), oder

3. bei der Daten im Sinne von Absatz 2 Nummer 3 und 4 durch den Einsatz technische Mittel gewonnen werden,

sind nur zulässig, soweit der Zweck der Maßnahme anders nicht erreicht oder die Zweckerreichung wesentlich erschwert wäre.

(4) Die Datenerhebung nach Absatz 1 Satz 1 darf nur auf eine Person gerichtet werden, bezüglich der Tatsachen die Annahme rechtfertigen,

1. dass sie als Verantwortliche in Anspruch genommen werden kann (§§ 218, 219) oder

2. dass sie vermisst oder suizidgefährdet ist oder sich in einer hilflosen Lage befindet, und die Bestimmung ihres Aufenthalts auf andere Weise aussichtslos oder wesentlich erschwert wäre.

Datenerhebungen nach Absatz 1 Satz 2 dürfen sich nur gegen die Person richten, deren individuelles Verhalten eine konkrete Wahrscheinlichkeit der Begehung einer terroristischen Straftat begründet.

(5) Die Datenerhebung ist nur hinsichtlich der Telekommunikationsanschlüsse zulässig, die von der in Absatz 3 genannten Person mit hoher Wahrscheinlichkeit genutzt werden oder von denen mit hoher Wahrscheinlichkeit mit ihnen Verbindung aufgenommen wird. Die Datenerhebung darf auch dann durchgeführt werden, wenn andere als die in Absatz 3 genannten Personen unvermeidbar betroffen werden. Daten anderer als in Absatz 3 genannter Personen dürfen bei Funkzellenabfragen und im Falle des Einsatzes technischer Mittel gemäß Absatz 3 Nummer 3 nur für einen Datenabgleich zur Ermittlung einer gesuchten Geräte- und Kartennummer verwendet werden und sind nach Beendigung der Maßnahme unverzüglich zu löschen.

(6) Jeder, der öffentlich zugängliche Telekommunikationsdienste anbietet oder an der Erbringung solcher Dienste mitwirkt, hat der Polizei die Überwachung und Aufzeichnung der Telekommunikation zu ermöglichen und die erforderlichen Auskünfte unverzüglich zu erteilen. Für eine Entschädigung der Diensteanbieter ist § 23 des Justizvergütungs- und -entschädigungsgesetzes vom 5. Mai 2004 (BGBl. I S. 718), zuletzt geändert durch Artikel 13 des Gesetzes vom 8. Dezember 2025 (BGBl. 2025 I Nr. 318) entsprechend anzuwenden, soweit nicht eine Entschädigung nach dem Telekommunikationsgesetz zu gewähren ist.“

11. § 185b Absatz 1 Satz 1 wird wie folgt gefasst:

„Die Polizei kann unter den Voraussetzungen des § 185a Absatz 1 von jedem Diensteanbieter verlangen, Kommunikationsverbindungen zu unterbrechen, zu verhindern oder die Verfügungsgewalt darüber in anderer geeigneter Weise zu entziehen.“

12. § 185c wird wie folgt geändert:

a) Absatz 1 Satz 2 wird wie folgt gefasst:

„Die Polizei darf unter den Voraussetzungen des § 185 Absatz 2 durch die Verwendung von Vertrauenspersonen personenbezogene Daten erheben.“

b) Absatz 3 wird wie folgt geändert:

aa) In Nummer 4 wird die Angabe „eingetragen ist, oder“ durch die Angabe „eingetragen ist,“ ersetzt.

bb) In Nummer 5 wird die Angabe „ein Verbotsverfahren betreibt.“ durch die Angabe „ein Verbotsverfahren betreibt, oder“ ersetzt.

cc) Nach Nummer 5 wird folgende Nummer 6 eingefügt:

„6. Mitglied der Führungsebene einer kriminellen oder einer terroristischen Vereinigung ist.“

c) Absatz 4 wird wie folgt geändert:

aa) In Nummer 4 wird die Angabe „Einfluss zu nehmen.“ durch die Angabe „Einfluss zu nehmen, oder“ ersetzt.

bb) Nach Nummer 4 wird folgende Nummer 5 eingefügt:

„5. als Mitglied der Führungsebene einer kriminellen Vereinigung oder einer terroristischen Vereinigung auf die Aktivitäten einer solchen Vereinigung Einfluss zu nehmen.“

13. Nach § 185c werden folgende §§ 185d und 185e eingefügt:

„**§ 185d**

Datenerhebung zur Abwehr unbemannter Fahrzeugsysteme

(1) Soweit dies zur Abwehr einer Gefahr für die öffentliche Sicherheit erforderlich ist, die von einem unbemannten Fahrzeugsystem ausgeht, das an Land, in der Luft oder

zu Wasser betrieben wird, kann die Polizei die dem unbemannten Fahrzeugsystem zuzuordnenden personenbezogenen Daten erheben und verarbeiten, insbesondere zur Feststellung der für den Betrieb und die Steuerung verantwortlichen Person, zur Ermittlung des Startplatzes des Fahrzeugsystems, zur Verfolgung seiner Bewegungsrichtung und zur Feststellung des Standorts des Fahrzeugsteuerers.

(2) Unter den Voraussetzungen des Absatzes 1 kann die Polizei vom Fahrzeugsteuerer ohne dessen Wissen Bildaufnahmen und -aufzeichnungen anfertigen, soweit dies zur Feststellung seiner Identität oder seines Standortes erforderlich ist. Eine Maßnahme nach Satz 1 darf auch durchgeführt werden, wenn Dritte von der Datenverarbeitung unvermeidbar betroffen sind. Für die Speicherung und Weiterverarbeitung der Bildaufnahmen und -aufzeichnungen gilt § 184 Absatz 6 entsprechend. Die Durchführung verdeckter Maßnahmen gemäß § 185 bleibt unberührt.“

„**§ 185e**

Datenerhebungen mittels mobiler Sensorträgersysteme

(1) Die Polizei kann zur Durchführung der in Satz 2 genannten Maßnahmen mobile Sensorträgersysteme verwenden, wenn die Voraussetzungen für die Erhebung personenbezogener Daten nach den Bezugsnormen jeweils vorliegen und die Verwendung mobiler Sensorträgersysteme in der Anordnung der Datenerhebung zugelassen ist. Maßnahmen im Sinne des Satzes 1 sind:

1. die Datenerhebung bei öffentlichen Veranstaltungen und Ansammlungen sowie an allgemein zugänglichen Orten gemäß § 184 Absatz 1 bis 5;

2. der Einsatz besonderer Mittel der Datenerhebung gemäß § 185 Absatz 1 Nummer 1 und 2 sowie Absatz 3;

3. die Datenerhebung durch Telekommunikationsüberwachung gemäß § 185a;

4. die Datenerhebung zur Abwehr unbemannter Fahrzeugsysteme gemäß § 185d.

(2) In den Fällen des Absatzes 1 Satz 2 Nummer 1 muss bei Einsatz eines mobilen Sensorträgersystems gewährleistet sein, dass die Erhebung der personenbezogenen Daten offen erfolgt; in diesem Fall soll auf die Verwendung mobiler Sensorträgersysteme gesondert hingewiesen werden.

(3) Wird bei einer Datenerhebung nach Absatz 1 ein unbemanntes Fahrzeugsystem als Sensorträger eingesetzt, darf dieses nur dann mit Mitteln des unmittelbaren Zwanges ausgerüstet sein, wenn die Datenerhebung mit einer Maßnahme gemäß § 213a verbunden ist.“

14. § 186 wird wie folgt geändert:

a) In Absatz 1 Nummer 6 werden nach der Angabe „die Überwachung der Telekommunikation“ die Wörter „und Erhebung von Verkehrsdaten“ eingefügt.

b) In Absatz 7 Satz 2 wird die Angabe „§ 185a Absatz 3 Satz 3“ durch die Angabe „§ 185a Absatz 5 Satz 2“ ersetzt.

15. § 186a wird wie folgt geändert:

a) Die Überschrift wird wie folgt gefasst:

„§ 186a Grundsätze der Datenverarbeitung bei Maßnahmen nach §§ 185, 185a und § 185c“

b) Die Absätze 1 bis 4 werden wie folgt gefasst:

„(1) Die Anordnung von Maßnahmen der Datenerhebung gemäß §§ 185, 185a und § 185c ist unzulässig, wenn tatsächliche Anhaltspunkte für die Annahme vorliegen, dass durch sie allein Daten aus dem Kernbereich privater Lebensgestaltung erlangt werden, oder die Art und Weise ihrer Durchführung in den Kernbereich eingreift. Die Art und Weise einer Datenerhebung greift in den Fällen des § 185 Absatz 1 Nummer 3 und § 185c insbesondere dann in den Kernbereich privater Lebensgestaltung ein, wenn ein Vertrauensverhältnis aufgebaut oder fortgeführt wird, dass intimen oder engsten persönlichen Beziehungen entspricht; das gilt auch, wenn ein bestehendes Vertrauensverhältnis dieser Art zur Datenerhebung genutzt wird. Vor der Durchführung von Maßnahmen nach §§ 185, 185a und § 185c ist durch technische Vorkehrungen und organisatorische Maßnahmen sicherzustellen, dass eine Verletzung des Kernbereichs privater Lebensgestaltung unterbleibt; von geeigneten Vorkehrungen und Maßnahmen darf nur dann abgesehen werden, wenn sie trotz des Gewichts des Eingriffs mit unverhältnismäßigem Aufwand verbunden wären.

(2) Laufende Maßnahmen nach §§ 185, 185a und § 185c sind, soweit tatsächliche Anhaltspunkte für die Annahme vorliegen, dass durch sie Inhalte aus dem Kernbereich privater Lebensgestaltung erfasst werden, oder die Art und Weise ihrer Durchführung in den Kernbereich eingreift, unverzüglich zu unterbrechen oder, soweit dies zur Vermeidung des Eindringens in den Kernbereich ausreicht, zu beschränken. Beim Einsatz von Personen zur verdeckten Datenerhebung gemäß § 185 Absatz 1 Nummer 3 und § 185c darf die Unterbrechung oder Beschränkung nach Satz 1 soweit und solange aufgeschoben werden, wie dies zur Vermeidung einer Gefahr für Leib oder Leben der eingesetzten Person unerlässlich ist. Ein Aufschub der Unterbrechung oder Beschränkung ist im Fall des Satzes 1 auch zulässig, soweit und solange durch sie die Verwendbarkeit der eingesetzten Person für weitere verdeckte

Datenerhebungen aufgrund bestimmter Tatsachen konkret gefährdet wäre. Bestehen bei einer Maßnahme nach § 185 Absatz 1 Nummer 2 Buchstabe a oder Buchstabe c oder bei einer Maßnahme nach § 185a während der Durchführung der Maßnahme hinsichtlich der Betroffenheit des Kernbereichs Zweifel, darf die Maßnahme im Wege der automatischen Aufzeichnung fortgesetzt werden. Nach einem Abbruch oder einer Beschränkung der Maßnahme gemäß Satz 1 sind die Maßnahme und die Art und Weise ihrer Durchführung nach Maßgabe von Absatz 1 erneut zu bewerten; sie darf nur fortgesetzt werden, soweit aufgrund tatsächlicher Anhaltspunkte anzunehmen ist, dass durch die Maßnahme Erkenntnisse, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, nicht erfasst werden.

(3) Daten, die durch Maßnahmen nach § 185 Absatz 3 erhoben wurden, sind dem zuständigen Gericht unverzüglich vorzulegen. Das gleiche gilt für Daten, die im Wege der automatischen Aufzeichnung nach Absatz 2 Satz 4 erhoben wurden. Das zuständige Gericht entscheidet unverzüglich über die Verwertbarkeit oder Löschung der Daten. Zuständig ist das Gericht, das die Maßnahme angeordnet hat, durch welche die Daten erhoben wurden, oder, wenn die Datenerhebung nicht auf einer gerichtlichen Anordnung beruht, das nach § 186 Absatz 6 Satz 1 zuständige Gericht. § 186 Absatz 6 Satz 2 bis 7 gelten entsprechend.

(4) Bei Gefahr im Verzug kann die Leiterin oder der Leiter des Landespolizeiamtes, des Landeskriminalamtes, einer Polizeidirektion oder eine von ihr oder ihm besonders beauftragte Person des Polizeivollzugsdienstes im Benehmen mit der oder dem behördlichen Datenschutzbeauftragten über die Verwertung der Erkenntnisse im Sinne des Absatzes 3 entscheiden. Die gerichtliche Entscheidung nach Absatz 3 ist unverzüglich nachzuholen.“

c) Nach Absatz 4 wird folgender Absatz 4a eingefügt:

„(4a) Ergibt sich bei der Auswertung von Daten, die durch Maßnahmen nach §§ 185, 185a oder § 185c erhoben wurden, dass sie Inhalte aus dem Kernbereich privater Lebensgestaltung betreffen, oder dass durch die Art und Weise der Durchführung der Maßnahme in den Kernbereich eingegriffen wurde, hat die Weiterverarbeitung unverzüglich zu unterbleiben. Beim Einsatz von Personen zur verdeckten Datenerhebung gemäß § 185 Absatz 1 Nummer 3 und § 185c sind die erlangten Erkenntnisse vor Weitergabe durch die eingesetzten Personen sowie durch deren polizeiliche Führungspersonen hinsichtlich ihrer Kernbereichsrelevanz zu überprüfen. Die Leiterin oder der Leiter des Landespolizeiamtes, des Landeskriminalamtes, einer Polizeidirektion oder eine von ihr oder ihm besonders beauftragte Person des Polizeivollzugsdienstes prüft im Benehmen mit der oder dem behördlichen Datenschutzbeauftragten die Verwertbarkeit, wenn

1. in den Fällen des Satzes 1 oder 2 Zweifel bestehen, ob die Daten wegen eines Eindringens in den Kernbereich privater Lebensgestaltung unverwertbar sind, oder

2. die Daten aus einer Maßnahme stammen, die nach Absatz 2 Satz 1 abgebrochen oder beschränkt wurde.

Verbleiben nach einer Prüfung gemäß Satz 3 Zweifel an der Verwertbarkeit, sind die Daten unverzüglich zu löschen. Anstelle der Löschung kann die Leiterin oder der Leiter des Landespolizeiamtes, des Landeskriminalamtes, einer Polizeidirektion oder eine von ihr oder ihm besonders beauftragte Person des Polizeivollzugsdienstes die gerichtliche Bestätigung der Verwertbarkeit beantragen; Absatz 3 und 4 gelten entsprechend."

d) Absatz 5 wird wie folgt gefasst:

„(5) Daten, die durch Maßnahmen nach §§ 185, 185a oder § 185c erhoben wurden und dem Kernbereich privater Lebensgestaltung zuzurechnen sind, dürfen nicht verwertet werden und sind unverzüglich zu löschen."

e) Nach Absatz 5 wird folgender Absatz 5a eingefügt:

„(5a) Bei Maßnahmen nach §§ 185, 185a und § 185c sind zu dokumentieren:

1. die Tatsache der Erhebung von Daten, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, und die Löschung der Daten aus diesem Grund;

2. die Unterbrechung oder Beschränkung einer Maßnahme und deren eventueller Aufschub sowie die Fortsetzung einer Maßnahme nach einer Unterbrechung oder Beschränkung einschließlich der jeweils tragenden Gründe;

3. die Entscheidung über die Verwertung von Erkenntnissen bei Gefahr im Verzug gemäß Absatz 4;

4. die Durchführung einer Prüfung nach Absatz 4a Satz 3 und ihr Ergebnis.

Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist sechs Monate nach der Benachrichtigung oder der Erteilung der gerichtlichen Zustimmung über das endgültige Absehen von der Benachrichtigung nach § 186 Absatz 7 und 8 zu löschen. Ist die Datenschutzkontrolle nach § 186b Absatz 1 noch nicht beendet, ist die Dokumentation bis zu ihrem Abschluss aufzubewahren." ‘

8. Die bisherigen Nummern 5, 6 und 7 werden zu Nummern 16, 17 und 18.

9. Nach dem Änderungsbefehl zur Einfügung von §§ 188c, 188b (neue Nummer 18) wird folgende Nummer 19 eingefügt:

‚**19. § 189 Absatz 1 Satz 4 wird wie folgt geändert:**

„Die Polizei kann darüber hinaus personenbezogene Daten, die sie im Rahmen von Strafermittlungsverfahren über eine Person gewonnen hat, die einer Straftat verdächtig ist, weiterhin in abrufbarer Weise verarbeiten, wenn Tatsachen, insbesondere die Art, Ausführung oder Schwere der Tat sowie die Persönlichkeit der tatverdächtigen Person, die Annahme rechtfertigen, dass die Person zukünftig Straftaten begehen wird, und die Datenverarbeitung zur Verhütung einer künftigen Straftat erforderlich ist.“ ‘

10. Die bisherigen Nummern 8, 9, 10, 11, 12 und 13 werden zu Nummern 20, 21, 22, 23, 24 und 25.

11. Nummer 14 wird wie folgt geändert:

a) Nummer 14 wird zu Nummer 26.

b) In § 201c Absatz 1 Satz 1 wird nach der Angabe „eine terroristische Straftat“ die Angabe „im Sinne von § 185a Absatz 1 Satz 3“ eingefügt.

b) § 201c Absatz 1 Satz 2 wird gestrichen.

12. Die bisherige Nummer 15 wird zu Nummer 27.

13. Nach dem Änderungsbefehl zur Einfügung von § 201d (neue Nummer 27) wird folgende Nummer 28 eingefügt:

‚**28. § 202 Absatz 2 wird wie folgt geändert:**

a) Nummer 2 wird wie folgt gefasst:

„2. wenn sie sich an einem Ort befindet, für den die in § 181 Absatz 1 Satz 2 Nummern 1 bis 4 genannten Voraussetzung vorliegen,“

b) Nummer 3 wird wie folgt gefasst:

„3. wenn sie sich an einem der in § 181 Absatz 1 Satz 2 Nummer 5 bezeichneten Orte aufhält und Tatsachen die Annahme rechtfertigen, dass die Durchsuchung zur Bekämpfung der grenzüberschreitenden Kriminalität oder zur Verhütung einer Straftat von erheblicher Bedeutung im Sinne jener Vorschrift erforderlich ist, oder“

c) Nach Nummer 3 wird folgende Nummer 4 eingefügt:

„4. wenn die Person nach § 187 oder nach dem Recht der Europäischen Union zur gezielten Kontrolle ausgeschrieben ist.“ ‘

14. Die bisherigen Nummern 16, 17 und 18 werden zu Nummern 29, 30 und 31.

15. Nach dem Änderungsbefehl zur Einfügung von § 205a (neue Nummer 31) werden folgende Nummern 32, 33 und 34 eingefügt:

‚**32. § 206 wird wie folgt geändert:**

a) In Nummer 6 wird der Punkt am Ende durch ein Komma ersetzt.

b) Nach Nummer 6 werden folgende Nummern 7 und 8 eingefügt:

„7. es sich um ein Fahrzeug handelt, in dem sich eine Person befindet, die nach § 202 Absatz 2 Nummer 3 durchsucht werden darf; die Durchsuchung kann sich auch auf die in dem Fahrzeug enthaltenen Sachen erstrecken.“

33. In § 206a wird die Angabe „Artikel 99 Schengener Durchführungsüberein- kommen vom 19. Juni 1990“ durch die Angabe „dem Recht der Europäischen Union“ ersetzt.

34. Nach § 213 wird folgender § 213a eingefügt:

„**§ 213a**

Maßnahmen gegen unbemannte Fahrzeugsysteme

(1) Soweit dies zur Abwehr einer Gefahr für die öffentliche Sicherheit, die von einem unbemannten Fahrzeugsystem ausgeht, das an Land, in der Luft oder zu Wasser betrieben wird, erforderlich ist, kann die Polizei technische Mittel und Mittel des unmittelbaren Zwangs einsetzen, um die Fernsteuerung zu unterbrechen, die Steuerung zu übernehmen, das unbemannte Fahrzeugsystem zu beschädigen oder zu zerstören oder in sonstiger Weise auf das unbemannte Fahrzeugsystem einzuwirken. Die Polizei kann zur Durchführung einer Maßnahme nach Satz 1 unbemannte Fahrzeugsysteme verwenden. Befugnisse zur Gefahrenabwehr nach dem Recht des Straßenverkehrs, des Luftverkehrs und der Schifffahrt bleiben unberührt.

(2) Eine Maßnahme nach Absatz 1 Satz 1 und 2 ist nicht zulässig, soweit durch sie ein Schaden für Rechtsgüter Dritter droht, der außer Verhältnis zu dem Schaden steht, der durch die Maßnahme abzuwehren ist.

(3) Die Polizei kann zur Erkennung einer Gefahr im Sinne des Absatzes 1 technische Mittel einsetzen. Die Befugnis zur Erhebung personenbezogener Daten nach anderen Vorschriften bleibt unberührt.“ ‘

16. Die bisherige Nummer 19 wird zu Nummer 35.

Begründung:

1. Zu Nummer 1 (Inhaltsübersicht)

Die Inhaltsübersicht ist aufgrund der Einführung der weiteren Vorschriften gemäß §§ 181b, 184d, 185d, 185e und § 213a LVwG-Entwurf sowie und der redaktionellen Änderung der Überschriften des § 185a und des § 186a LVwG anzupassen.

2. Zu Nummer 2 (Änderung von § 179 LVwG und § 180a LVwG)

a) Änderung des § 179 LVwG

aa) Einführung von § 179 Absatz 6 LVwG-Entwurf

Mit § 179 Absatz 6 LVwG-Entwurf wird eine Rechtsgrundlage für die Erhebung und Weiterverarbeitung von Standortdaten aus geografischen Koordinatensystemen geschaffen, die automatisiert und ohne Interaktion der anrufenden Person anfallen, wenn insbesondere mit einem Smartphone eine Notrufverbindung zu einer polizeilichen Notrufeinrichtung hergestellt wird. Die Polizei wird durch diese Rechtsgrundlage zur Nutzung des AML-Dienstes berechtigt. AML steht hier für Advanced Mobile Location als quelloffener Dienst zur Positionsbestimmung von Anrufern bei der Nutzung einer Notrufnummer. Mit dieser Art von Technologie kann der Standort der Anruferin oder des Anrufers schnell und sicher mit einer hohen Genauigkeit lokalisiert werden. Verbunden sind mit ihr deutliche Vorteile gegenüber der Ermittlung von Standortdaten auf der Grundlage von § 185a Absatz 2 Satz 2 LVwG über die Feststellung des Antennensystems der Funkzelle, in die ein mobiles Endgerät eingewählt ist. Die Möglichkeit zur Ermittlung des Standortes kann von großer Bedeutung sein, wenn eine in Not geratene Person nicht in der Lage ist ihren Standort mitzuteilen.

Die Polizei ist gemäß § 179 Absatz 6 **Satz 1** LVwG-Entwurf befugt, die im Rahmen der Herstellung einer Notrufverbindung zu einer polizeilichen Notrufeinrichtung anfallenden Standortdaten, etwa mittels des AML-Dienstes, zu erheben und vorübergehend zu speichern. Zu einer darüber hinausgehenden Verarbeitung dieser Daten ist sie befugt,

wenn dies zur Abwehr einer Gefahr erforderlich ist. Es geht hier um Fälle, in denen die Person, die die Notrufverbindung durch die Anwahl des Notrufs hergestellt hat, physisch oder psychisch nicht in der Lage ist, ihren Standort mitzuteilen, weitere polizeiliche Maßnahmen aber notwendig sind. In diesen Fällen darf die Polizei die erhobenen Standortdaten auswerten und zum Anlass für weitere Maßnahmen nehmen. Von der Eingriffsschwelle umfasst ist auch der sogenannte Gefahrenverdacht, also eine Situation, in der trotz verständiger Würdigung der vorliegenden Tatsachen und Kenntnisse zweifelhaft ist, ob eine Gefahr besteht. Hier dürfen die Daten für einen sogenannten Gefahrerforschungseingriff verarbeitet werden, um abzuklären, ob eine Gefahr vorliegt.

Gemäß § 179 Absatz 6 **Satz 2** LVwG-Entwurf in Verbindung mit § 179 Absatz 5 Satz 2 LVwG sind die erhobenen Daten grundsätzlich spätestens einen Monat nach dem Speicheranlass zu löschen. Es handelt sich hierbei um eine Höchstfrist. Die Speicherfrist im Rahmen des AML-Dienstes ist tatsächlich wesentlich kürzer. Die Daten werden für derzeit 60 Minuten zum Abruf durch eine polizeiliche Notrufeinrichtung verschlüsselt vorgehalten. Nach 60 Minuten werden die Daten automatisch und endgültig gelöscht. Die Löschverpflichtung besteht jedoch nicht, wenn die Daten aus repressiven oder präventiven Gründen zweckändernd weiterverarbeitet werden.

§ 179 Absatz 6 **Satz 3** LVwG-Entwurf stellt klar, dass im Einzelfall die Erhebung von Telekommunikationsdaten nach Maßgabe des § 185a LVwG zulässig ist.

bb) Einführung von § 179 Absatz 7 LVwG-Entwurf

Die Richtlinie (EU) 2019/882 vom 17. April 2019 über die Barrierefreiheitsanforderungen für Produkte und Dienstleistungen (ABl. L 151, S. 70) findet keine unmittelbare Anwendung auf die nationale Notrufnummer 110. Es ist gleichwohl sachgerecht, auch für diese Notrufnummer – wie für die Notrufnummer 112 (vgl. § 8 der Landesverordnung zur Durchführung des Schleswig-Holsteinischen Rettungsdienstgesetzes) – die rechtlichen Grundlagen für einen barrierefreien Betrieb zu schaffen. § 179 Absatz 7 LVwG-Entwurf ermächtigt dementsprechend das für Inneres zuständige Ministerium durch Rechtsverordnung vorzuschreiben, welchen Anforderungen die Notrufnummer 110 genügen muss, damit sie auch von Menschen mit Behinderungen genutzt werden kann.

b) Änderung von § 180a Absatz 4 LVwG

§ 180a Absatz 4 LVwG normiert Abfragebefugnisse der Polizei zur Erhebung von Bestands- und Nutzungsdaten bei Anbietern digitaler Dienste, also Unternehmen, die digitale Dienste zur Verfügung stellen, wie Plattformen, Onlineshops, Vermittlungsdienste, Suchmaschinen und soziale Netzwerke. Die Vorschrift ist an die Umfirmierung des Gesetzes anzupassen, das die Übermittlungsbefugnisse und Pflichten der Anbieter digitaler Dienste regelt. Dieses Telekommunikation-Telemedien-Datenschutz-Gesetz (TDDDG) vom 23. Juni 2021 (BGBl. I S. 1982; ber. BGBl. I 2022 S. 1045) wurde bereits mit Wirkung zum 14. Mai 2024 in Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz umbenannt (BGBl. 2024 I Nr. 149).

3. Zu Nummer 3 (Anpassung der Nummerierung der Drs. 20/4284)

Der Änderungsantrag bedingt eine Änderung der Nummernfolge der Änderungsbefehle der Drs. 20/4284. Die bisherige Nummer 2 wird zur Nummer 4.

4. Zu Nummer 4 (Einführung eines § 181b LVwG-Entwurf und Änderung von § 183 LVwG)

a) Einführung eines § 181b LVwG-Entwurf

aa) Einführung einer allgemein-polizeilichen Befugnis für Kontrollen in den Küstengewässern

§ 181b LVwG-Entwurf bezweckt den Schutz wesentlicher Infrastruktureinrichtungen oder anderer Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen im Küstenmeer und in den inneren Gewässern.

Das **Küstenmeer** bezeichnet einen an die Landfläche eines Küstenstaates angrenzenden Meeresstreifen, in dem der Küstenstaat seine Souveränität ausübt (Hoheitsgewässer); es umfasst ausgehend von einer sogenannten Basislinie maximal zwölf Seemeilen (etwa 22,224 Kilometer). Der Rechtsrahmen des Küstenmeeres wird maßgeblich durch den Abschnitt 2 des Seerechtsübereinkommens der Vereinten Nationen (SRÜ) geprägt. Mit **inneren Gewässern** sind die landeinwärts zur Basislinie des Küstenmeeres gelegenen Gewässer bezeichnet (Artikel 8 SRÜ).

Im deutschen Küstenmeer und in den landeinwärts der Basislinie gelegenen inneren Gewässern nehmen die Wasserschutzpolizeien sowohl die allgemein-polizeilichen Aufgaben als auch die schifffahrtspolizeilichen Vollzugsaufgaben wahr (Graulich in: Schenke/Graulich/Ruthig, 2. Aufl. 2018, BPolG § 6 Rn. 36). Letztere Aufgaben erfüllt die Landespolizei auf der Grundlage der Vereinbarung über die Ausübung der schifffahrtspolizeilichen Vollzugsaufgaben vom 14. Dezember 1954 (ratifiziert durch Gesetz vom 15. Juli 1955, GVOBl. Schl.-H. S. 137). Es handelt sich um die auftragsweise Wahrnehmung einer Bundesaufgabe durch Behörden des Landes im Wege der Organleihe (Kment in: Jarass/Pieroth, 18. Aufl. 2024, GG, Art. 89 Rn. 4). Dies hat zur Folge, dass die Wasserschutzpolizei in diesem Aufgabensegment ausschließlich Bundesrecht anwendet (Ehlers, SeeAufgG, 6. Aufl. 2023, § 3 Rn. 7). Die allgemein-polizeilichen Aufgaben nimmt die Wasserschutzpolizei dagegen auf der Basis des Polizeirechts des Landes wahr. Dieses enthält allerdings aktuell keine spezifischen Befugnisse zur Erfüllung der allgemein-polizeilichen Vollzugsaufgaben im Küstenmeer.

§ 181b LVwG-Entwurf schließt diese Lücke mit dem Ziel, die Abklärung bestimmter Sachlagen, die auf Gefährdungen hindeuten, zu ermöglichen und damit die Effektivität der Gefahrenabwehr im maritimen Raum jenseits der schifffahrtspolizeilichen Aufgaben der Wasserschutzpolizei zu stärken. Auch im Küstenmeer und in den inneren Gewässern hat die **Gewährleistung der Sicherheit von Infrastruktureinrichtungen** vor dem Hintergrund der spätestens durch den russischen Angriffskrieg auf die Ukraine deutlich veränderten Sicherheitslage in Europa an Bedeutung gewonnen. Dies gilt insbesondere für Schleswig-Holstein mit seiner einzigartigen geografischen Lage. Diese Entwicklungen begründen die Gefahr, dass maritime Räume, in denen sich eine Vielzahl von wichtigen Infrastruktureinrichtungen wie Unterseedatenkabel, Energieversorgungspipelines, Offshore-Windenergie-Anlagen, Ölplattformen und Brücken befinden, verstärkt Ziel von Ausforschungs- und Sabotagehandlungen werden können. Angesichts der Bedeutung der genannten Anlagen und Einrichtungen für das Gemeinwesen erscheinen niedrigschwellige Kontrollmöglichkeiten zur Verhütung von Schädigungen erforderlich. Die Landespolizei soll befähigt werden, anlassbezogen verdächtige Wasserfahrzeuge respektive verdächtige Aktivitäten auf beziehungsweise von Wasserfahrzeugen zu überprüfen, Risiken aufzuklären und – wenn sich Hinweise auf Schädigungshandlungen verdichten – erforderlichenfalls einzuschreiten.

Das Land kann § 181b LVwG als Standardbefugnis auf Grundlage der **Gesetzgebungskompetenz** gemäß Artikel 70 Absatz 1 GG erlassen. Die Regelungsmaterie fällt nicht in die konkurrierende Gesetzgebungskompetenz des Bundes gemäß Artikel 74 Absatz 1 Nummer 21 GG. In ihrer Zusammenschau bilden die in diesem Kompetenztitel enthaltenen Regelungsmaterien der Hochseeschifffahrt, der Küstenschifffahrt, der Seezeichen und der Binnenschifffahrt das Recht des Wasserverkehrs. Charakteristisch für diese Materie ist sein Verkehrsbezug, der die Gesetzgebungszuständigkeit auch begrenzt (Uhle in: Dürig/Herzog/Scholz,

108. EL August 2025, GG, Art. 74 Rn. 494, 498). Zu dieser Regelungsmaterie gehört auch die Abwehr spezifischer Gefahren der Seeschifffahrt und damit die Schifffahrtspolizei (Uhle a. a. O. Rn. 503). Nicht erfasst sind Normen des Gefahrenabwehrrechts, die sich zwar auf den Wasserverkehr auswirken, aber keine verkehrsspezifische Gefahr abwehren.

Die Unterbindung von Sabotagehandlungen respektive entsprechende Vorbereitungshandlungen, wie das Auskundschaften von Objekten, stellt nicht schon deswegen die Abwehr einer wasserverkehrsspezifischen Gefahr dar, weil die gefahrbegründenden Handlungen von Schiffen oder Booten aus erfolgen. Dasselbe gilt insofern, als ein Schiff oder Boot dem Transport zu einem Tatort dient. Die Nutzung von Wasserfahrzeugen resultiert hier vielmehr aus der Lage der Schutzobjekte oder der Tarnung der Tathandlung. Eine wasserverkehrsspezifische Gefahr kommt erst in Betracht, wenn über den rein instrumentellen Bezug der Gefahr zu einem Wasserfahrzeug hinaus die Gefahr aus der Eigenschaft des Wasserfahrzeuges folgt, zum Beispiel indem es selbst bewusst missbraucht wird, um geschützte Einrichtungen oder Anlagen zu beschädigen. In solchen Fällen kann sich ein Anwendungsvorrang des Schifffahrtspolizeirechts ergeben. § 181b Absatz 1 Satz 3 LVwG stellt dies klar.

bb) Recht auf friedliche Durchfahrt

Die Ausübung der durch § 181b LVwG-Entwurf vorgesehenen Befugnisse steht im Einklang mit dem Recht auf friedliche Durchfahrt nach Artikel 17 ff. SRÜ. Das völkerrechtlich gewährleistete Recht auf friedliche Durchfahrt garantiert Schiffen fremder Flagge die ungehinderte Durchfahrt des Küstenmeeres, solange die Passage friedlich erfolgt.

Voraussetzung der **Durchfahrt** im Sinne des Artikel 18 SRÜ ist, dass sie zügig und ununterbrochen und mit dem Ziel des Passierens des Küstenmeeres durchgeführt wird. Unterbrechungen oder Ankerungen sind nur aus zwingenden navigationsbedingten Gründen und soweit es üblicherweise zur Schifffahrt gehört oder bei Notlagen beziehungsweise in Fällen höherer Gewalt zulässig (Stopps zum Schlafen, Picknicken oder Baden sind nicht erlaubt).

Jede Durchfahrt im Sinne des SRÜ muss **friedlich** sein. Die Friedlichkeit der Durchfahrt wird, solange sie den Frieden oder die Sicherheit des Küstenstaates nicht beeinträchtigt, unterstellt. Gewisse Tätigkeiten eines Schiffes machen eine Durchfahrt jedoch unabweislich unfriedlich. Diese Handlungen finden sich im Katalog des Artikel 19 Absatz 2 Buchstabe a bis l SRÜ; folgende dort genannte Tätigkeiten sind von Relevanz im Zusammenhang mit dem Schutz von wesentlichen Infrastruk-

tureinrichtungen oder Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen:

- eine Handlung, die auf das Sammeln von Informationen zum Schaden der Verteidigung oder Sicherheit des Küstenstaats gerichtet ist;

- das Starten, Landen oder Anbordnehmen von Luftfahrzeugen;

- eine Handlung, die auf die Störung eines Nachrichtenübermittlungssystems oder anderer Einrichtungen oder Anlagen des Küstenstaats gerichtet ist;

- alle Tätigkeiten, die nicht unmittelbar mit der Durchfahrt zusammenhängen.

Der Küstenstaat wird insbesondere durch letztgenannte Auffangvorschrift von der Pflicht entbunden, im konkreten Einzelfall nachzuprüfen, ob eine Beeinträchtigung des Friedens, der Ordnung oder der Sicherheit des Küstenstaats vorliegt (Graf Vitzthum, HdB Seerecht, 1. Aufl. 2006, S. 124). Andererseits sind stets konkrete Handlungsweisen erforderlich. Eine abstrakte Feststellung der Unfriedlichkeit von vornherein, etwa wegen einer bestimmten Ladung, ist nicht zulässig.

Soweit Tatsachen vorliegen, die auf eine Gefahr für wesentliche Infrastruktureinrichtungen oder sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen hindeuten – etwa ständige Kurswechsel, Absetzen von Fahrzeugen oder Gegenständen ins Wasser (AUV = Autonomous Underwater Vehicles), Decksarbeiten an verdächtigen Aufbauten, Drohnenabflüge von oder -landungen auf dem Schiff, Tauchgänge jeweils in Verbindung mit bestimmten Lageerkenntnissen – entfällt der Schutz der friedlichen Durchfahrt und die Landespolizei ist befugt, auf Grundlage des Gefahrenabwehrrechts Schleswig-Holsteins angemessene Maßnahmen zu ergreifen (Artikel 25 Absatz 1 SRÜ).

Solange nicht feststeht, ob eine Durchfahrt im Sinne des Artikel 18 SRÜ vorliegt oder ob die Durchfahrt aufgrund konkreter Handlungen als unfriedlich im Sinne des Artikel 19 Absatz 2 SRÜ zu qualifizieren ist, sind die Maßnahmen auf solche zu beschränken, die der Aufklärung des Sachverhaltes, der Gefahrenvorsorge und der Risikobewertung dienen. Dabei ist der Grundsatz der Verhältnismäßigkeit in besonderem Maße zu beachten, um eine faktische Beeinträchtigung oder Vereitelung zulässiger Durchfahrten zu vermeiden.

Erst wenn feststeht, dass keine Durchfahrt im Sinne des Artikel 18 SRÜ vorliegt oder dass die Durchfahrt aufgrund konkreter Handlungen als unfriedlich im Sinne des Artikel 19 Absatz 2 SRÜ zu qualifizieren ist, können weitergehende Maßnahmen ergriffen werden. In diesen Fällen besteht kein Schutz durch das Recht der friedlichen Durchfahrt. Auch

intensivere Eingriffe sind dann zulässig, soweit sie erforderlich und angemessen sind. Die Norm trägt damit dem Spannungsverhältnis zwischen der Wahrung völkerrechtlich garantierter Durchfahrtsrechte und dem legitimen Interesse des Staates an einer präventiven Gefahrenabwehr im Küstenmeer Rechnung.

cc) Zu § 181b Satz 1 LVwG-Entwurf

§ 181b Absatz 1 Satz 1 LVwG-Entwurf ermächtigt die Polizei zu einer Kontrolle von Wasserfahrzeugen bei Vorliegen von Tatsachen, die die Annahme rechtfertigen, dass die Kontrolle zur Abwehr einer Gefahr für wesentliche Infrastruktureinrichtungen oder Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen erforderlich erscheint.

Die Vorschrift eröffnet ein hinsichtlich der Eingriffsschwere abgestuftes Vorgehen:

- Die Polizei wird bei Vorliegen der Tatbestandsvoraussetzungen zunächst ermächtigt, das Wasserfahrzeug, einschließlich der Betriebs- und Geschäftsräume, zu betreten und in Augenschein zu nehmen.

- Anzuhalten ist das Wasserfahrzeug nur, soweit dies für die Ausübung der Betretungsbefugnis oder der Befugnis zur Inaugenscheinnahme erforderlich ist.

- Soweit dies im Einzelfall erforderlich erscheint, darf die Polizei auch die Identität von Personen feststellen, die sich auf dem Wasserfahrzeug befinden.

Ein Einschreiten auf Grundlage von § 181b erfordert, dass bestimmte Tatsachen vorliegen, die nicht bloß abstrakt, sondern konkret die Möglichkeit begründen, dass die Kontrolle erforderlich ist, um eine Gefahr für das Schutzgut „wesentliche Infrastruktureinrichtung oder Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen“ abzuwehren. Durch diese Einschreitschwelle wird sichergestellt, dass die Kontrolle einerseits nur **anlassbezogen** erfolgen darf. Andererseits muss eine konkrete Gefahr – also die hinreichende Wahrscheinlichkeit des Eintritts eines Schadens im konkreten Einzelfall – für das genannte Rechtsgut noch nicht vorliegen. Die Polizei wird vielmehr zur Gefahrenvorsorge berechtigt. Das heißt die Kontrollbefugnis verfolgt das Ziel – soweit bestimmte Tatsachen auf eine Gefahrenlage hindeuten – das spätere Entstehen der Gefahr zu verhindern oder zumindest deren wirksame Bekämpfung zu ermöglichen.

Das **Schutzgut** des § 181b LVwG sind „wesentliche Infrastruktureinrichtung oder Anlage mit unmittelbarer Bedeutung für das Gemeinwe-

sen“. Dieses Rechtsgut zählt das BVerfG zu den besonders gewichtigen Rechtsgütern (vgl. BVerfG, Urt. v. 16. Feb. 2023, 1 BvR 1547/19 pp. = BVerfGE 165, 363 [410] Rn. 105 m. w. N.). Der Kreis der geschützten Anlagen und Einrichtungen ist polizeirechtlich autonom zu bestimmen. Eine Orientierung liefern die einschlägigen Rechtsakte der EU, namentlich die RL (EU) 2022/2557 und die RL (EU) 2022/2555, und ihre nationale Umsetzung. Mithin stehen Betriebsstätten oder technische Installationen im Fokus, mit denen die Versorgung der Allgemeinheit in bestimmten Sektoren (Energie, Wasser, Gesundheitswesen, Ernährung, Informationstechnik, Telekommunikation usw.) gewährleistet wird. Anders als für den wirtschaftsrechtlichen KRITIS-Begriff der vorgenannten Regelungskomplexe kommt es für das polizeirechtliche Schutzgut nicht auf bestimmte Schwellenwerte (Zahl der potentiell betroffenen Versorgungseinheiten und Personen) an. Erforderlich ist jedoch, dass ein Ausfall oder eine Störung sich über den privaten Bereich hinaus auf das gesellschaftliche Zusammenleben auswirkt, sei es, weil das Ausmaß der Rechtsgutsbeeinträchtigungen nach Anzahl der Betroffenen oder ihrer Intensität hoch einzuschätzen ist oder weil das Vertrauen in staatliche Aufgabenerfüllung erschüttert wäre. Auch andere Regelungskomplexe können zur Bestimmung des Schutzbereiches herangezogen werden. Dies gilt etwa für den Begriff der lebenswichtigen und verteidigungswichtigen Einrichtungen im Sinne von § 2 Absatz 2 LSÜG. Durch letztere sind auch Schlüsselbetriebe der Rüstungs- und Verteidigungsindustrie und solche Betriebe dieses Sektors, denen eine besondere „betriebliche Eigengefahr“ anhaftet, sowie Telekommunikationsunternehmen erfasst (Däubler, 1. Aufl. 2019, SÜG [Bund], § 1 Rn. 31).

dd) Zu § 181b Satz 2 LVwG-Entwurf

Die Schwelle für die Befugnis zur Betretung und Inaugenscheinnahme hebt § 181b Absatz 1 Satz 2 LVwG-Entwurf für Zeiträume an, die außerhalb der Betriebs- und Geschäftszeiten liegen. In diesem Fall muss die polizeiliche Maßnahme der Verhütung einer dringenden Gefahr im Sinne von Artikel 13 Absatz 7 Alternative 3 GG dienen. Unter dieser Voraussetzung ermöglicht § 181b Absatz 1 Satz 2 LVwG-Entwurf auch die Betretung von Wohnräumen.

ee) Zu § 181b Satz 3 LVwG-Entwurf

§ 181b Absatz 1 Satz 3 LVwG-Entwurf grenzt die landesrechtliche Kontrollbefugnis des allgemeinen Gefahrenabwehrrechts gegenüber den schifffahrtspolizeilichen Vollzugsaufgaben ab. Das spezielle Gefahrenabwehrrecht genießt grundsätzlich Vorrang.

Die Aufgaben der Schifffahrtspolizei teilen sich nach Maßgabe von § 1 Nummer 2 des Seeaufgabengesetzes (SeeAufgG) im Wesentlichen in die Bereiche „Abwehr von Gefahren für die Sicherheit und Leichtigkeit des Verkehrs“ sowie „Verhütung von der Seeschifffahrt ausgehender Gefahren und schädlicher Umwelteinwirkungen“. Der Begriff der „Sicherheit und Leichtigkeit des Verkehrs“ im Sinne von § 1 Nummer 2 SeeAufgG ist weit zu verstehen. Unter die Leichtigkeit des Verkehrs fällt der reibungslose, unbehinderte Ablauf desselben (Ehlers, SeeAufgG, 6. Aufl. 2023, § 1 Rn. 16). Zur Sicherheit des Verkehrs gehört die eigentliche Verkehrssicherheit, die durch falsches Verhalten im Verkehr gefährdet werden kann. Sie ist hierauf aber nicht beschränkt. Auch Gefahren, die von einem Schiff, seiner Ladung oder von Personen an Bord ausgehen und zu Beeinträchtigungen des Schiffsverkehrs führen können, werden erfasst. Ebenso zählt auch die Abwehr äußerer Gefahren (wie Terroranschläge oder Piratenangriffe auf Schiffe) zur Verkehrssicherheit. Zusammenfassend gehören zur Sicherheit und Leichtigkeit des Verkehrs alle Maßnahmen, die dazu dienen, dass ein Schiff ohne sich selbst oder andere zu gefährden, und ohne Verzögerungen und Behinderungen am Schiffsverkehr teilnehmen kann (zum Ganzen: Ehlers, SeeAufgG, 6. Aufl. 2023, § 1 Rn. 16).

b) Änderung von § 183 LVwG

aa) Neufassung von § 183 Absatz 1 Satz 3 LVwG

§ 183 LVwG regelt die Befugnis der Polizei, eine erkennungsdienstliche Behandlung durchzuführen. Gemäß § 183 Absatz 1 Satz 1 LVwG ist dies zulässig, wenn eine Identitätsfeststellung auf andere Weise nicht oder nur unter erheblichen Schwierigkeiten möglich ist. Darüber hinaus gestattet § 183 Absatz 1 Satz 3 LVwG erkennungsdienstliche Behandlungen auch dann, wenn eine Person bestimmter Straftaten im Sinne des § 179 Absatz 2 LVwG dringend verdächtig ist und eine Wiederholungsgefahr besteht. De lege lata darf diese erkennungsdienstliche Behandlung „zur Verhütung oder Aufklärung einer künftigen Straftat“ erfolgen. Das Schleswig-Holsteinische Verwaltungsgericht hat jedoch mit Urteil vom 21. Dezember 2022 (3 A 291/20) erhebliche Zweifel an der formellen Verfassungsmäßigkeit der zweiten Alternative („zur Aufklärung einer künftigen Straftat“) geäußert (BeckRS 2022, 37925). Die insoweit landesrechtlich normierte Strafverfolgungsvorsorge sei durch die in die konkurrierende Gesetzgebung des Bundes fallende Vorschrift des § 81b Absatz 1 Alternative 2 der Strafprozessordnung (StPO) vollständig verdrängt. Nach eingehender Prüfung ist dieser Rechtsauffassung zu folgen und die kritische Tatbestandsalternative zu streichen, zumal andere Bundesländer diesen Schritt seit längerem vollzogen haben (vgl. OVG Lüneburg, Beschl. v. 16. Sep. 2009, 11 ME 402/09).

Darüber hinaus werden die normativen Vorgaben für die Prognoseentscheidung des Absatzes 1 Satz 3 mit den Prognosekriterien des § 189 Absatz 1 Satz 4 LVwG harmonisiert, um eine höhere systematische Kohärenz zwischen den Vorschriften zu erreichen. § 183 Absatz 1 Satz 3 LVwG und die in § 189 Absatz 1 Satz 4 LVwG normierte Befugnis, sogenannte „Kriminalakten“ anzulegen, bilden die wichtigsten Fälle des Gefahrenabwehrrechts des Landes zur vorsorgenden Speicherung von personenbezogenen Daten, die aus Strafverfahren stammen.

bb) Einfügung eines § 183 Absatz 2a LVwG-Entwurf

§ 183 Absatz 2a LVwG-Entwurf trägt zunächst dem Umstand Rechnung, dass der Abgleich biometrischer Daten, die aus erkennungsdienstlich erhobenen Daten gewonnen wurden, in der Praxis bereits genutzt wird. Die Änderung dient insoweit lediglich der Klarstellung und der Herstellung von Transparenz hinsichtlich dieser Datenverarbeitung. Die enge Zweckbindung dieser Datenverarbeitung an die Identifizierung im Rahmen der erkennungsdienstlichen Behandlung rechtfertigt es, die Regelung in § 183 LVwG zu verorten.

Zugleich schafft § 183 Absatz 2a LVwG-Entwurf die rechtlichen Voraussetzungen, einen nach § 195 LVwG zulässigen Abgleich in den Fällen des § 183 Absatz 1 Satz 1 LVwG um die ergänzende Abfrage des gemeinsamen Speichers für Identitätsdaten nach den Verordnungen (EU) 2019/817 und (EU) 2019/818 zu erweitern. Die Interoperabilitätsarchitektur dient der schnellen und sicheren systemübergreifenden Identifizierung, dem unionsweiten biometrischen Abgleich und der Aufdeckung von Mehrfachidentitäten. Die Vorschrift eröffnet keinen allgemeinen Zugriff auf unionsrechtliche Datenbestände, sondern begrenzt die ergänzende Abfrage auf den unionsrechtlich vorgesehenen Zweck der Identifizierung einer anwesenden Person. Voraussetzung ist, dass einer der in den Artikeln 20 der Verordnungen (EU) 2019/817 und (EU) 2019/818 geregelten Identifizierungsanlässe vorliegt, die Maßnahme zwingend erforderlich ist und die erlangten Daten ausschließlich zu diesem Zweck verarbeitet werden dürfen. § 183 Absatz 2a LVwG-Entwurf erweitert damit in eng begrenzten Fällen den für die Identifizierung verfügbaren Datenbestand, wenn die Identität der betroffenen Person mit anderen Mitteln nicht oder nur unter erheblichen Schwierigkeiten festgestellt werden kann.

cc) Änderung von § 183 Absatz 3 LVwG

Es handelt sich um eine redaktionelle Anpassung. Die einschlägigen, bei der Durchführung der erkennungsdienstlichen Behandlung anfallen-

den Unterlagen können auch in elektronischer Form vorliegen, sodass es sprachlich treffender erscheint, neben ihrer Vernichtung auch ihre etwaige Löschung vorzuschreiben.

5. Zu Nummer 5 (Anpassung der Nummerierung der Drs. 20/4284)

Der Änderungsantrag bedingt eine Änderung der Nummernfolge der Änderungsbefehle der Drs. 20/4284. Die bisherige Nummer 3 wird zur Nummer 7.

6. Zu Nummer 6 (Änderungen von Nummer 4 der Drs. 20/4284)

a) Anpassung der Nummerierung der Drs. 20/4284

Der Änderungsantrag bedingt eine Änderung der Nummernfolge der Änderungsbefehle der Drs. 20/4284. Die bisherige Nummer 4 wird zur Nummer 8.

b) Änderung des Änderungsbefehls

In den Änderungsbefehl ist die Einfügung von § 184d LVwG-Entwurf aufzunehmen.

c) Einführung von § 184d LVwG-Entwurf

Durch diesen Änderungsantrag werden mit der Einführung von § 184d LVwG-Entwurf die rechtlichen Grundlagen für die Nutzung moderner technischer Systeme im öffentlichen Verkehrsraum zur automatisierten **Feststellung von Ablenkungsverstößen** geschaffen.

Die Ablenkung durch elektronische Geräte kann Ursache schwerer Verkehrsunfälle sein. Verstöße gegen das straßenverkehrsrechtliche Verbot zur Nutzung elektronischer Geräte durch Fahrzeugführende (§ 23 Absatz 1a der Straßenverkehrsordnung / StVO) bleiben häufig unentdeckt. An Aktionstagen durchgeführte Schwerpunktkontrollen, Unfallanalysen und wissenschaftliche Studien weisen auf eine erhebliche Dunkelziffer hin. Mit herkömmlichen Kontrollmethoden lässt sich das verbotswidrige Verhalten nicht im erforderlichen Maße erfassen. Demgegenüber bieten moderne technische Systeme die Mög-

lichkeit, Bildaufzeichnungen automatisiert auf Muster auszuwerten, die auf eine unerlaubte Benutzung von elektronischen Geräten hindeuten. Der Einsatz entsprechender Technik erfordert allerdings eine bereichsspezifische Rechtsgrundlage (AG Trier, Urt. v. 2. März 2023, 2 OWi 8113 Js 1906/23 = DAR 2023, 338 [340]). Ziel ist es, durch wirksame Kontrollmechanismen Fahrzeugführende, die sich rechtswidrig verhalten, aus der Anonymität herauszuheben und zu identifizieren, um damit durch Generalprävention Gefahren für das Leben und die Gesundheit anderer Verkehrsteilnehmerinnen und Verkehrsteilnehmer vorzubeugen.

aa) Gesetzgebungskompetenz

Das Land kann die Standardbefugnisse gemäß § 184d LVwG-Entwurf auf Grundlage von Artikel 70 Absatz 1 GG erlassen. Ihre Einführung fällt nicht in eine Bundeskompetenz; soweit Berührungspunkte zur konkurrierenden Bundeskompetenz für den Straßenverkehr bestehen, entfaltet das Bundesrecht keine Sperrwirkung.

Artikel 74 Absatz 1 Nummer 1 GG ordnet die **Regelungsmaterie gerichtliches Verfahren** der konkurrierenden Gesetzgebung des Bundes zu. Die auf dieser Grundlage erlassenen Bundesvorschriften zum Strafverfahrens- und Ordnungswidrigkeitenrecht würden dann eine Sperrwirkung gegenüber den mit diesem Änderungsantrag vorgesehenen Datenerhebungsbefugnissen entfalten, wenn diese als Regelungen des Strafprozessrechts beziehungsweise des Rechts des Ordnungswidrigkeitenverfahrens zu beurteilen wären. Das ist jedoch nicht der Fall.

Ob eine Vorschrift die Straf- beziehungsweise Ordnungswidrigkeitenverfolgung oder die Gefahrenabwehr regelt, richtet sich nach deren Zielsetzung, wie sie sich in objektivierter Sicht aus ihrer Ausgestaltung ergibt. Gefahrenabwehr und Straf- beziehungsweise Ordnungswidrigkeitenverfolgung liegen oft nahe beieinander. Die Regelungsbefugnisse von Bund und Ländern können sich insoweit überschneiden. Dabei ist auch möglich, dass Regelungen doppelfunktional ausgerichtet sind und sowohl der Verfolgung von Straftaten und Ordnungswidrigkeiten als auch der Gefahrenabwehr dienen. Bei doppelfunktionalen Maßnahmen, bei denen sich ein eindeutiger Schwerpunkt weder im präventiven noch im repressiven Bereich ausmachen lässt, steht dem Gesetzgeber ein Entscheidungsspielraum für die Zuordnung zu. Entsprechende Befugnisse können unter Umständen sowohl auf Bundes- als auch auf Landesebene geregelt werden. Der Landesgesetzgeber ist folglich nicht an dem Erlass einer der Gefahrenabwehr dienenden Regelung gehindert, weil diese ihren tatsächlichen Wirkungen nach auch Interessen der Straf- oder Ordnungswidrigkeitenverfolgung dient und damit Regelungsbereiche des Bundes berührt (zum Ganzen instruktiv: BVerfG, Beschl. 18. Dez. 2018, 1 BvR 142/15 = BVerfGE 150, 244 [272 ff.] Rn. 63 ff.). Die Möglichkeit, doppelfunktionale Maßnahmen vorzusehen, enthebt al-

lerdings nicht von der Notwendigkeit, die Kompetenzen sorgfältig abzuschichten und die Ausgestaltung der Regelungen strikt von der Zwecksetzung her zu bestimmen.

Gemäß diesen Vorgaben verfolgt die automatisierte Datenerhebung im öffentlichen Verkehrsraum zur Erkennung von Ablenkungsverstößen Zwecke der **Gefahrenabwehr**. Die automatisierte Datenerhebung im öffentlichen Verkehrsraum zur Erkennung von Ablenkungsverstößen zielt darauf, gefährliche Ablenkungen einer Fahrzeugführerin oder eines Fahrzeugführers durch eine verbotswidrige Benutzung elektronischer Geräte zu unterbinden. Damit dient die Datenerhebung und -verarbeitung, zu der sie ermächtigt, der Abwehr von Gefahren für das Leben und die Gesundheit von Verkehrsteilnehmerinnen und Verkehrsteilnehmern (s. auch AG Trier, Urt. v. 2. März 2023, 2 OWi 8113 Js 1906/23 = DAR 2023, 338 [344]). Der gefahrenabwehrende Zweck wird über die generalpräventive Wirkung der Überwachungsmaßnahme insofern erreicht, als Fahrzeugführerinnen und Fahrzeugführer, die sich rechtswidrig verhalten, aus der Anonymität herausgehoben und identifiziert werden. Durch die Möglichkeit wirksamer Kontrollen kann ein insgesamt höheres Maß an normenkonformem Verhalten bewirkt werden. Es geht mithin nicht um eine repressiv-personenbezogene Verfolgung von Rechtsverstößen, sondern um den präventiv-objektiven Schutz der Integrität der Rechtsordnung und der durch sie geschützten Rechtsgüter. Dass im Ergebnis zugleich die Verfolgung von Ordnungswidrigkeiten befördert wird, ist nach den dargestellten Maßstäben unschädlich.

Die Zuständigkeit des Bundes zur **Regelung des Straßenverkehrs** (Artikel 74 Absatz 1 Nummer 22 GG) steht der Einführung der Vorschriften ebenfalls nicht entgegen. Dieser Kompetenztitel betrifft das Straßenverkehrsrecht als sachlich begrenztes Ordnungsrecht. Das Straßenverkehrsrecht dient dem Zweck, die spezifischen Gefahren, Behinderungen und Belästigungen auszuschalten oder wenigstens zu mindern, die mit der Straßennutzung unter den Bedingungen des modernen Verkehrs verbunden sind (vgl. nur: Kment in: Jarass/Pieroth, 18. Aufl. 2024, GG, Art. 74 Rn. 61; Uhle in: Dürig/Herzog/Scholz, 108. EL Aug. 2025, GG, Art. 74 Rn. 526, 528). Zwar ist nicht von der Hand zu weisen, dass die automatisierte Datenerhebung zur Aufdeckung von Ablenkungsverstößen gemäß § 184d LVwG-Entwurf, die unmittelbar an das Verbot aus § 23 Absatz 1a der StVO anknüpft, als Abwehr von Gefahren bewertet werden könnte, die sich gerade aus dem Betrieb von Kraftfahrzeugen ergeben. Die Zuordnung zur Gesetzgebungsmaterie des Straßenverkehrsrechts kann jedoch im Ergebnis offen bleiben. Denn der Bundesgesetzgeber hat von seiner Gesetzgebungskompetenz aus Artikel 74 Absatz 1 Nummer 22 GG in Bezug auf die Verkehrsüberwachung nicht abschließend Gebrauch gemacht (zur Geschwindigkeitsüberwachung durch eine sogenannte Abschnittskontrolle: OVG Lüneburg, Beschl. v. 3. Juli 2019, 12 MC 93/19 = NJW 2019, 2951 [2953] Rn. 22; BVerwG, Beschl. v. 31. Juli 2020, 3 B 4/20 = NVZ 2021, 99 Rn. 13). Die Bundeskompetenz entfaltet insoweit keine Sperrwirkung (Artikel 72 Absatz 1 GG).

bb) Einführung von § 184d LVwG-Entwurf

§ 184d Absatz 1 LVwG-Entwurf regelt den Umfang und grundlegende Modalitäten der Datenerhebung und Datenverarbeitung beim Einsatz technischer Systeme zur automatisierten Erkennung von Ablenkungsverstößen von Fahrzeugführerinnen und Fahrzeugführern. Die Datenerhebung ist auf den öffentlichen Verkehrsraum beschränkt, also auf Örtlichkeiten, die aufgrund entsprechender straßenverkehrsrechtlicher Widmung Verkehrszwecken dienen und an denen Straßenverkehr stattfindet.

Zweck der Datenerhebung und -verarbeitung ist gemäß § 184d Absatz 1 **Satz 1** LVwG-Entwurf die Verhütung der unerlaubten Nutzung elektronischer Geräte durch Fahrzeugführende. Sie dient damit der Verhinderung von Rechtsgutsverletzungen und -gefährdungen – namentlich der körperlichen Unversehrtheit und des Lebens anderer Verkehrsteilnehmerinnen und Verkehrsteilnehmer – die mit dem pflichtwidrigen Verhalten verbunden sein können.

§ 184d LVwG-Entwurf knüpft insoweit an die Regelung des § 23 Absatz 1a StVO an. Gemäß dieser Vorschrift darf, wer ein Fahrzeug führt, elektronische Geräte zur Kommunikation, Information oder Organisation – wie etwa Mobiltelefone oder Autotelefone, Berührungsbildschirme, tragbare Flachrechner, Navigationsgeräte – nur benutzen, wenn hierfür das Gerät weder aufgenommen noch gehalten wird und entweder eine Sprachsteuerung und Vorlesefunktion genutzt wird oder zur Bedienung und Nutzung des Gerätes nur eine kurze, den Umständen angepasste Blickzuwendung zum Gerät (bei gleichzeitig entsprechender Blickabwendung vom Verkehrsgeschehen) erfolgt und erforderlich ist.

§ 184d LVwG-Entwurf gestattet zur Erreichung des gefahrenabwehrenden Zwecks den Einsatz von Technik, mit der wirksam Verstöße gegen § 23 Absatz 1a StVO automatisiert erkannt werden können. Ziel ist es, durch das Erkennbar-machen der Verstöße ein pflichtgemäßes Verhalten der Fahrzeugführerinnen und Fahrzeugführer zu bewirken. Dementsprechend schreibt § 184d Absatz 1 Satz 1 LVwG-Entwurf vor, dass der Technikeinsatz offen zu erfolgen hat, das heißt, dass er im Einzelfall kenntlich zu machen ist.

Im Einzelnen wird die Polizei gemäß § 184d Absatz 1 **Satz 2** LVwG-Entwurf ermächtigt, Bildaufzeichnungen von einzelnen Fahrzeugen und Fahrzeugführenden anzufertigen und das Kennzeichen des Fahrzeuges zu erfassen. Die Bildaufzeichnungen der Fahrzeugführenden dürfen sodann mit Hilfe bildverarbeitender Systeme auf Muster hin automatisiert ausgewertet werden, die auf eine unerlaubte Benutzung von elektronischen Geräten hindeuten. Außerdem können Ort, Zeit und Fahrtrichtung des Fahrzeuges dokumentiert werden.

Datenerhebung und Datenverarbeitung auf Grundlage von § 184d LVwG-Entwurf stellen **Eingriffe in das Recht auf informationelle Selbstbestimmung** dar (vgl. AG Trier, Urt. v. 2. März 2023, 2 OWi 8113 Js 1906/23 = DAR 2023, 338 [339]). Ihnen ist ein erhebliches Eingriffsgewicht zuzumessen. Folgende Gesichtspunkte sind zu berücksichtigen: Das Eingriffsgewicht wird durch den Umstand gemindert, dass die Bildaufzeichnungen nur im öffentlichen Verkehrsraum stattfinden und offen erfolgen. Überdies ist zu berücksichtigen, dass sie gegenüber der ganz überwiegenden Zahl der Betroffenen mit keinerlei unmittelbar beeinträchtigenden Folgen verbunden ist und keine Spuren hinterlässt. Ins Gewicht fällt dagegen, dass Bildaufzeichnungen der das Fahrzeug führenden Person angefertigt und ausgewertet werden müssen, um eine eventuelle unerlaubte Nutzung elektronischer Geräte zu erkennen. Erhöhend auf das Eingriffsgewicht wirkt sich ferner aus, dass sich die Maßnahme auf eine unbestimmte Vielzahl von Personen erstreckt, die von vornherein hierzu keinerlei Anlass gegeben haben.

Der Eingriff ist verfassungsrechtlich gerechtfertigt, weil er einen legitimen Zweck verfolgt und zur Erreichung dieses Zwecks geeignet, erforderlich und verhältnismäßig im engeren Sinne ist. Gegenüber der herkömmlichen auf einzelne Fahrzeuge beschränkte Kontrollen durch Polizeikräfte, ermöglicht der Einsatz der technischen Systeme die Feststellung von Ablenkungsverstößen deutlich effektiver. Der von § 184d LVwG-Entwurf verfolgte Zweck steht auch nicht außer Verhältnis zum Eingriffsgewicht. Dem erheblichen Eingriffsgewicht entsprechend verfolgt die Datenerhebungs- und -verarbeitungsbefugnis dem Schutz von Rechtsgütern von (mindestens) erheblichem Gewicht, nämlich Leben und Gesundheit in einer straßenverkehrsspezifischen Gefahrensituation (vgl. AG Trier, Urt. v. 2. März 2023, 2 OWi 8113 Js 1906/23 = DAR 2023, 338 [344]). Zwar knüpft § 184d LVwG-Entwurf nicht an eine konkrete Gefahrenlage an. Jedoch kann auch ein gefährliches oder risikobehaftetes Tun respektive die Beherrschung besonderer Gefahrenquellen Anknüpfungspunkt einer Kontrollmaßnahme sein. Die Rechtfertigung ergibt sich hier aus der besonderen Verantwortung gegenüber der Allgemeinheit. Dies hat das BVerfG gerade in Bezug auf Datenerhebungen im öffentlichen Straßenverkehr resp. für Gefahren, die sich aus dem Betrieb von Kraftfahrzeugen ergeben, anerkannt (siehe: BVerfG, Beschl. 18. Dez. 2018, 1 BvR 142/15 = BVerfGE 150, 244 [282] Rn. 94). Schließlich stehen Art und Intensität der Grundrechtsbeeinträchtigung zu den den Eingriff legitimierenden Anlässen in einem angemessenen Verhältnis. Dies ist dadurch gewährleistet, dass § 184d Absatz 1 Satz 1 LVwG nur zu einem stichprobenweisen Einsatz der Technik ermächtigt und damit eine flächendeckende Überwachung ausschließt (dazu: BVerfG, Beschl. 18. Dez. 2018, 1 BvR 142/15 = BVerfGE 150, 244 [285] Rn. 100).

Der **Begriff der Stichprobe** bezieht sich bei § 184d Absatz 1 Satz 1 LVwG-Entwurf insbesondere auf die Auswahl von Kontrollorten und Kontrollzeiträumen. Das heißt stichprobenweise erfolgt die Datenerhebung, wenn sie auf vorab festgelegte, räumlich und zeitlich begrenzte

Kontrollorte und Kontrollzeiträume beschränkt ist. Nicht verlangt ist eine zusätzliche Auswahl einzelner Fahrzeuge innerhalb des festgelegten Kontrollfensters. Eine Stichprobe im Sinne der Vorschrift liegt daher nicht erst dann vor, wenn innerhalb des Kontrollfensters nur die nach einem vorher festgelegten abstrakten Kriterium ausgewählten Fahrzeuge (zum Beispiel jedes vierte oder zehnte Fahrzeug) erfasst oder ausgewertet wird. Maßgeblich ist vielmehr die räumliche und zeitliche Begrenzung der Maßnahme. Die Auswahl der Einsatzzeiten und -orte ist planmäßig, anhand objektiver Kriterien zu treffen.

Ein Einsatz der automatisierten Datenerhebung und -verarbeitung zur Erkennung von Ablenkungsverstößen, der über Stichproben hinaus geht, ist gemäß § 184d Absatz 1 **Satz 3** LVwG-Entwurf nur zulässig, wenn dokumentierte polizeiliche Lageerkenntnisse dies erforderlich erscheinen lassen. Diese können sich beispielsweise aus einer vergleichsweise hohen Zahl erkannter Verstöße oder aus der Unfallstatistik ergeben. Damit wird sichergestellt, dass die Maßnahme an konkrete Anlässe und nachvollziehbare Erkenntnisse gebunden bleibt.

§ 184d Absatz 1 **Satz 4** LVwG-Entwurf stellt klar, dass die Datenerhebung auch durchgeführt werden darf, wenn Dritte unvermeidbar betroffen werden, etwa wenn im Einzelfall zufällig neben der das Fahrzeug führenden Person andere Fahrzeuginsassinnen und -insassen von den Bildaufzeichnungen erfasst werden.

bb) Zu § 184d Absatz 2 und 3 LVwG-Entwurf

§ 184d Absatz 2 und 3 LVwG-Entwurf formulieren die Grundregeln für die weitere Verwendung der erhobenen Daten:

Eine Weiterverarbeitung der nach § 184d Absatz 1 LVwG-Entwurf erhobenen Daten ist nur unter den in § 184d **Absatz 2 Satz 1** LVwG-Entwurf formulierten Bedingungen zulässig: Erstens muss durch die automatisierte Auswertung der Bildaufzeichnungen ein Muster erkannt worden sein, dass auf eine unerlaubte Nutzung elektronischer Geräte hindeutet. Zweitens muss die (hieran anschließende) unverzügliche Überprüfung der Bildaufzeichnung durch qualifizierte Beschäftigte der Polizei einen Verstoß gegen § 23 Absatz 1a StVO bestätigt haben. Nur unter diesen zwei Bedingungen ist gemäß § 184d **Absatz 2 Satz 2** LVwG-Entwurf eine Weiterverarbeitung der Daten zulässig. Sind sie erfüllt, ist auch eine Speicherung der erhobenen Daten nach Maßgabe der Vorschriften über das Ordnungswidrigkeitenverfahren gestattet, soweit sich der Anfangsverdacht einer Ordnungswidrigkeit bestätigt. Rechtsgrundlage ist hierfür § 100h Absatz 1 Satz 1 Nummer 1 StPO in Verbindung mit § 46 Absatz 1 des Ordnungswidrigkeitengesetzes. Vor beziehungsweise bis zur Bestätigung des Verstoßes darf das betroffene Fahrzeug gegebenenfalls gemäß § 184d **Absatz 2 Satz 3** LVwG-Entwurf ange-

halten werden. § 184d **Absatz 3** LVwG-Entwurf verpflichtet zur sofortigen, technisch spurenlosen Löschung der erhobenen Daten, wenn eine der Bedingungen von § 184d Absatz 2 Satz 1 LVwG-Entwurf nicht erfüllt ist. Die Löschung erfolgt automatisiert, um eine manuelle Nachbearbeitung auszuschließen und die sofortige Umsetzung sicherzustellen.

cc) Zu § 184d Absatz 4 LVwG-Entwurf

§ 184d Absatz 3 LVwG-Entwurf regelt das Protokollierungsverfahren. Bei Vorliegen eines technischen „Treffers“ – also in Fällen, in welchen durch die automatisierte Auswertung der Bildaufzeichnungen ein Muster erkannt worden ist, dass auf eine unerlaubte Nutzung elektronischer Geräte hindeutet – ist gemäß § 184d Absatz 4 **Satz 1** LVwG-Entwurf eine Protokollierung entsprechend § 186c LVwG vorgesehen. Sie umfasst Anlass, Ergebnis und Zeitpunkt der Löschung und ermöglicht eine datenschutzrechtliche und fachaufsichtliche Überprüfung der Maßnahme. In allen anderen Fällen schließt § 184d Absatz 4 **Satz 2** LVwG-Entwurf dagegen eine personenbezogene Protokollierung aus. Stattdessen wird ein technisches Systemprotokoll ohne Personenbezug geführt, das lediglich die technischen Abläufe dokumentiert, insbesondere Zeitpunkte und Verarbeitungsvorgänge einschließlich der Löschungen. Damit wird eine nachträgliche Kontrolle der Systemfunktion ermöglicht, ohne neue personenbezogene Daten zu erzeugen. Die im Allgemeinen in § 186b Absatz 1 LVwG geregelten Stichprobenkontrollen durch den oder die Landesbeauftragte für Datenschutz überträgt § 184d Absatz 4 **Satz 3** LVwG-Entwurf auf das spezifische Protokollierungsverfahren des § 184d Absatz 3 Satz 1 und 2 LVwG-Entwurf.

dd) Zu § 184d Absatz 5 LVwG-Entwurf

§ 184d Absatz 3 **Satz 1** LVwG-Entwurf setzt die aus dem Verhältnismäßigkeitsgrundsatz abzuleitenden Anforderungen in Bezug auf Transparenz und individuellen Rechtsschutz durch die Vorgabe um, die wesentlichen Entscheidungsgrundlagen der Anordnung einer automatisierten Datenerhebung zur Erkennung von Ablenkungsverstößen zu dokumentieren.

§ 184d Absatz 3 **Satz 2 und 3** LVwG-Entwurf weist die Polizei im Falle des Einsatzes eines Hochrisiko-KI-Systems im Sinne der Verordnung (EU) 2024/1689 auf ihre Betreiberpflichten nach europäischem Recht hin.

7. Zu Nummer 7 (Änderung von §§ 185, 185a, 185b, 185c LVwG, Einführung von §§ 185d und 185e LVwG-Entwurf sowie Änderung von §§ 186 und 186a LVwG)

a) Änderung von § 185 LVwG

aa) Neufassung des § 185 Absatz 2 LVwG

§ 185 Absatz 2 LVwG normiert, unter welchen Voraussetzungen die Polizei besondere Mittel der Datenerhebung einsetzen kann. Besondere Mittel der Datenerhebung sind:

- die (längerfristige) Observation,
- der verdeckte Einsatz technischer Mittel (zur Anfertigung von Bildaufzeichnungen/-aufnahmen, zur Ermittlung von Standort und Bewegung einer Person oder Sache, zum Abhören und Aufzeichnen des nichtöffentlich gesprochenen Wortes) sowie
- der Einsatz verdeckter Ermittler.

Erforderlich ist, dass Tatsachen dafür sprechen, dass ein Schaden für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit oder ein gleich gewichtiger Schaden für Sach- oder Vermögenswerte oder für die Umwelt zu erwarten ist und die Maßnahme zur Aufklärung des Sachverhalts unerlässlich ist.

Die seit Einführung der Vorschrift 1992 (GVOBl. Schl.-H S. 290) insoweit im Wesentlichen unverändert gebliebene Vorschrift setzt keine konkrete Gefahr voraus (vgl. Martens in: PdK SH A-15, LVwG § 185 Anm. 5). Die Vorverlagerung ist insoweit legitim, als das BVerfG derart eingriffsintensive verdeckte Maßnahmen unter der Voraussetzung einer **hinreichend konkretisierten Gefahr** für besonders gewichtige Rechtsgüter für gerechtfertigt erachtet (grundlegend: BVerfG, Urt. 20. Apr. 2016, 1 BvR 966/09 pp. = BVerfGE 141, 220 [272 f.] Rn. 112; ferner: BVerfG, Beschl. 9. Dez. 2022, 1 BvR 1345/21 = BVerfGE 165, 1 [49 f.] Rn. 90 f.).

Den Ausgangspunkt für diese Eingriffsschwelle bildet die in der Entscheidung des BVerfG vom 20. April 2016 (1 BvR 966/09 pp. = BVerfGE 141, 220) zum Bundeskriminalamtsgesetz aufgestellte Maxime, dass der Gesetzgeber von Verfassungs wegen nicht von vornherein für jede Art der Aufgabenwahrnehmung auf die Schaffung von Eingriffstatbeständen beschränkt ist, die dem tradierten sicherheitsrechtlichen Modell der Abwehr konkreter, unmittelbar bevorstehender oder gegenwärtiger Gefahren entsprechen. Vielmehr kann er die Grenzen für be-

stimmte Bereiche mit dem Ziel schon der Straftatenverhütung auch weiter ziehen, indem er die Anforderungen an die Vorhersehbarkeit des Kausalverlaufs reduziert (BVerfG a. a. O. [272 f.] Rn. 112). Eine solche – gegenüber der konkreten Gefahr abgegrenzte – hinreichend konkretisierte Gefahr in diesem Sinne kann danach schon bestehen, wenn sich der zum Schaden führende Kausalverlauf noch nicht mit hinreichender Wahrscheinlichkeit vorhersehen lässt, sofern bereits bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen. Erforderlich ist dafür im Grundsatz, dass Tatsachen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, das eine relevante Rechtsgutsverletzung verkörpert; des Weiteren muss über die Identität der betroffenen Personen so viel bekannt sein, dass die Überwachungsmaßnahme gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden kann (BVerfG a. a. O.; ferner: BVerfG, Beschl. v. 9. Dez. 2022, 1 BvR 1345/21 = BVerfGE 165, 1 [49 ff.] Rn. 90 f.).

Der geltende § 185 **Absatz 2** LVwG erfüllt die Anforderungen dieser Rechtsprechung des BVerfG an die Normierung einer hinreichend konkretisierten Gefahr als Voraussetzung für eingriffsintensive verdeckte Maßnahmen nicht in jeder Hinsicht und ist insoweit zu reformieren: Dabei ist zunächst der Eingriffsanlass (die sogenannte Eingriffsschwelle) dahingehend zu präzisieren, dass ein gattungsmäßig konkretisierbares Geschehen absehbar ist, das eine konkrete Gefahr für die Schutzgüter bedeutet.

Des Weiteren muss der Schutz in Bezug auf **besonders gewichtige Rechtsgüter** nachgeschärft werden. Zu diesen zählen „vor allem Leib, Leben und Freiheit der Person sowie Bestand oder Sicherheit des Bundes oder eines Landes“ (BVerfG, Urt. v. 16. Feb. 2023, 1 BvR 1547/19 pp. = BVerfGE 165, 363 [410] Rn. 105).

Auch die – bisher nicht erfasste – sexuelle Selbstbestimmung einer Person ist hierzu zu rechnen. Menschliches Verhalten mit sexueller Zielrichtung genießt über Artikel 2 Absatz 1 i. V. m. Artikel 1 Absatz 1 GG einen besonderen Autonomieschutz. Dem Einzelnen steht hiernach das Recht zur Selbstbestimmung zu, in welcher Einstellung er zum Geschlechtlichen steht oder in welcher Form er sein Sexualleben ausrichtet. Die öffentliche Gewalt bereitet dafür eine interessenausgleichende Rechtsordnung (Di Fabio in: Dürig/Herzog/Scholz, 108. EL August 2025, GG, Art. 2 Absatz 1 Rn. 200). Demgemäß kann zur Auslegung insbesondere der 13. Abschnitt im Besonderen Teil des Strafgesetzbuches (StGB) herangezogen werden (vgl. die Begründung der Aufnahme dieses Schutzgutes ins GewSchG durch das Gesetz zur Fortentwicklung der Strafprozessordnung und zur Änderung weiterer Vorschriften vom 25. Juni 2021, BT-Drs. 19/27654, 127). Im Strafrecht versteht man unter dem Recht auf sexuelle Selbstbestimmung das Abwehrrecht des Einzelnen, nicht gegen seinen Willen zum Objekt sexueller Annäherung durch andere gemacht zu werden. Gemeint ist das Recht einer Person,

über Zeit, Ort, Form und Partner sexueller Betätigung frei zu entscheiden (vgl. etwa Renikowski in: MüKo, StGB, 5. Aufl. 2025, StGB Vor § 174 Rn. 7 ff.). Wie beim Schutz der körperlichen Integrität („Leib“) erfährt der Schutzbereich eine erforderliche Einschränkung dadurch, dass dem Schutzgut ein „Angriff von erheblicher Intensität oder Auswirkung“ drohen muss.

Der Schutz von Sach- und Vermögenswerten erreicht nach Ansicht des BVerfG im Verhältnis zu den genannten besonders gewichtigen Rechtsgütern „ein vergleichbares Gewicht“ nur in Bezug auf Gegenstände, „deren Erhaltung im öffentlichen Interesse geboten ist, sofern darunter einem engen Verständnis folgend etwa wesentliche Infrastruktureinrichtungen oder sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen gefasst werden“ (BVerfG, Urt. v. 16. Feb. 2023, 1 BvR 1547/19 pp. = BVerfGE 165, 363 [410] Rn. 105). In dem letztgenannten Punkt ist der Kreis der geschützten Rechtsgüter entsprechend einzuschränken. Zur Bestimmung der geschützten Anlagen und Einrichtungen wird auf die Begründung zu § 181b LVwG-Entwurf verwiesen.

Der Eingriffstatbestand des § 185 Absatz 2 LVwG erfährt durch die Anpassung an die vorstehend dargestellte Rechtsprechung zur Eingriffsschwelle der hinreichend konkretisierten Gefahr notwendigerweise eine Beschränkung hinsichtlich des Kreises der geschützten Rechtsgüter im Bereich des Sach- und Vermögensschutzes und des Schutzes der Umwelt. Ein umfassender Schutz dieser Rechtsgüter ist im Vorfeld konkreter Gefahren nicht umsetzbar. Sie fallen gleichwohl damit nicht aus dem Schutzbereich. Erforderlich ist jedoch in Bezug auf diese Rechtsgüter die Einschreitschwelle anzuheben. Daher gestattet der Tatbestand des § 185 Absatz 2 LVwG künftig neben einer hinreichend konkretisierten Gefahr für besonders gewichtige Rechtsgüter den Einsatz besonderer Mittel der Datenerhebung auch bei einer **gegenwärtigen erheblichen Gefahr**. Eine erhebliche Gefahr ist eine Gefahr für „ein bedeutsames Rechtsgut“. Erfasst werden neben den besonders gewichtigen Rechtsgütern auch nicht unwesentliche Vermögenswerte sowie andere strafrechtlich geschützte Güter von vergleichbarem Gewicht zählen (Bäcker in: Lisken/Denninger/Bäcker PolR-HdB, 8. Aufl. 2026, Kap. 3 Rn. 120). Voraussetzung des Einschreitens für diese Schutzgüter ist jedoch eine konkrete Gefahr, die durch eine große zeitliche Nähe und einen gesteigerten Grad der Wahrscheinlichkeit des Schadenseintritts gekennzeichnet ist; gefordert ist eine Sachlage, bei der das schädigende Ereignis bereits begonnen hat oder in allernächster Zeit mit an Sicherheit grenzender Wahrscheinlichkeit bevorsteht (Bäcker a. a. O. Rn. 124).

bb) Streichung von § 185 Absatz 3 Satz 2 LVwG

§ 185 Absatz 3 regelt den Einsatz technischer Mittel zur Erhebung von personenbezogenen Daten in oder aus Wohnungen, also die akusti-

sche und optische Überwachung von Wohnräumen auf Grundlage von Artikel 13 Absatz 4 GG.

Der verdeckte Einsatz technischer Mittel zur Datenerhebung in und aus Wohnungen hat innerhalb der eingriffsintensiven verdeckten Maßnahmen ein besonders hohes Eingriffsgewicht. Daher bleibt der Kreis der geschützten Rechtsgüter ungeachtet der Neugestaltung des § 185 Absatz 2 LVwG auf einen Kernbestand der besonders gewichtigen Rechtsgüter beschränkt.

§ 185 Absatz 3 **Satz 2** LVwG wird gestrichen. Das BVerfG hat in seiner Entscheidung zum Sicherheits- und Ordnungsgesetz Mecklenburg-Vorpommerns vom 9. Dezember 2022 (1 BvR 1345/21) dargelegt, dass die Grundrechtsschranken aus Artikel 13 Absatz 4 und 5 GG für den präventiven Einsatz technischer Mittel in Wohnungen keine Eingriffe bei Vorliegen einer sogenannten hinreichend konkretisierten Gefahr gestatten (s. BVerfG a. a. O. = BVerfGE 165, 1 [68f.] Rn. 124 ff.). Prima facie scheint Absatz 3 Satz 2 diese Vorgabe (mit der Formulierung: „[e]ine dringende Gefahr kann […] auch darin bestehen [...]“) zwar zu erfüllen, der Sache nach ist hier jedoch eine an der sogenannten hinreichend konkretisierten Gefahr (siehe: Begründung zur Neufassung des § 185 Absatz 2 LVwG) orientierte Gefahrenschwelle „eigener Art“ normiert.

b) Neufassung des § 185a LVwG

Die Befugnis zur Telekommunikationsüberwachung wird mit unterschiedlicher Zielrichtung insgesamt neu gefasst.

Zunächst sind dabei die durch das LVwGPORÄndG vom 26. Februar 2021 eingeführten Eingriffsvoraussetzungen zur Abwehr terroristischer Gefahrenlagen zu nennen, deren Ausgestaltung an die fortentwickelte Rechtsprechung des Bundesverfassungsgerichts zur hinreichend konkretisierten Gefahr angepasst wird.

Des Weiteren wird eine Befugnis der Landespolizei zur Erhebung von Verkehrsdaten in § 185a Absatz 2 LVwG wieder eingeführt. Verkehrsdaten sind Daten, deren Erhebung, Verarbeitung oder Nutzung bei der Erbringung eines Telekommunikationsdienstes erforderlich sind (§ 3 Nummer 70 des Telekommunikationsgesetzes / TKG). Durch das Gesetz zur Änderung polizei- und ordnungsrechtlicher Vorschriften im Landesverwaltungsgesetz (LVwGPORÄndG) vom 26. Februar 2021 wurde die Vorschrift § 185a Absatz 2 Nummer 2 LVwG gestrichen, die bis dahin festgelegt hatte, dass sich eine Überwachung der Telekommunikation auch auf Verkehrsdaten erstrecken konnte. Ziel der Streichung war es, eine Fehlverweisung auf eine durch Entscheidung des

BVerfG (Urt. v. 2. März 2010, 1 BvR 256 pp. = BVerfGE 120, 260) bereits 2010 für nichtig erklärte Übermittlungsbefugnis (§ 113a TKG a. F.) in Bezug auf Verkehrsdaten zu berichtigen, die Telekommunikationsdiensteanbieter aufgrund einer gesetzlichen Speicherfrist vorzuhalten hatten (sogenannte Vorratsdatenspeicherung). Allerdings erfasste die Streichung unbeabsichtigt auch die Befugnis zur Erhebung solcher Verkehrsdaten, die von Telekommunikationsunternehmen regelmäßig und rechtmäßig nur kurzfristig zu betrieblichen und vertraglichen Zwecken gespeichert werden. Auf die Verfügbarkeit dieser Daten kann die Polizei jedoch angewiesen sein, insbesondere um Gefahren von vermissten Personen abzuwenden.

Überdies setzt der Änderungsantrag verschiedene Klarstellungen und Präzisierungen zum Umfang und den Grenzen der gefahrenabwehrenden Überwachung der Telekommunikation um.

aa) Änderung der Überschrift des § 185a LVwG

Mit der Wiedereinführung einer Befugnis zur Verkehrsdatenerhebung wird die Überschrift klarstellend angepasst.

bb) Zu § 185a Absatz 1 LVwG

§ 185a Absatz 1 LVwG normiert die Voraussetzungen für die Erhebung von Telekommunikationsdaten durch die Polizei zur Gefahrenabwehr. Die Vorschrift enthält zwei unterschiedliche Eingriffstatbestände. § 185a Absatz 1 Satz 1 LVwG gestattet die Datenerhebung, soweit sie zur Abwehr einer dringenden Gefahr für besonders gewichtige Rechtsgüter gemäß § 185 Absatz 2 Satz 2 LVwG-Entwurf erforderlich ist. § 185a Absatz 1 Satz 2 LVwG knüpft an terroristische Gefahrenlagen an.

Die Befugnis zur Telekommunikationsüberwachung gemäß § 185a Absatz 1 **Satz 1** LVwG weist seit ihrer Einführung 2007 (GVOBl. Schl.-H. S. 237) eine höhere Eingriffsschwelle auf als der Einsatz besonderer Mittel der Datenerhebung. Bis 2021 war eine gegenwärtige Gefahr gefordert; das Gesetz zur Änderung polizei- und ordnungsrechtlicher Vorschriften im Landesverwaltungsgesetz (LVwGPORÄndG) vom 26. Februar 2021 (GVOBl. Schl.-H. S. 237) hat an deren Stelle eine dringende Gefahr gesetzt (a. a. O. S. 227). Dieser (verfassungsrechtlich an sich nicht gebotene) Abstand der Eingriffsschwellen bleibt gewahrt. Eine Angleichung erfolgt indes in Bezug auf die Schutzgüter. Ein sachlicher Grund, bei der Überwachung der Telekommunikation von den besonders gewichtigen Rechtsgütern im Sinne von § 185 Absatz 2 Satz 2 LVwG-Entwurf bestimmte Rechtsgüter vom Schutz auszunehmen, ist nicht ersichtlich.

Der mit dem LVwGPORÄndG vom 26. Februar 2021 eingeführte § 185a Absatz 1 **Satz 2** LVwG erfasst Gefahrenlagen durch terroristische Straftaten. Im Rahmen seiner mit der Entscheidung vom 20. April 2016 (1 BvR 966/09 u. a.) zum BKAG begründeten Rechtsprechung hat das BVerfG in Bezug auf terroristische Straftaten eine spezielle Ausprägung der hinreichend konkretisierten Gefahr entwickelt (zum Begriff der hinreichend konkretisierten Gefahr siehe: Begründung zur Neufassung des § 185 Absatz 2 LVwG-Entwurf). Speziell in Bezug auf terroristische Straftaten, die oft durch lang geplante Taten von bisher nicht straffällig gewordenen Einzelnen an nicht vorhersehbaren Orten und in ganz verschiedener Weise verübt werden, können die Anforderungen an die Erkennbarkeit des Geschehens weiter abgesenkt werden, wenn dafür bereits genauere Erkenntnisse über die beteiligten Personen bestehen. Hier gilt, dass Überwachungsmaßnahmen auch dann erlaubt werden können, wenn zwar noch nicht ein seiner Art nach konkretisiertes und zeitlich absehbares Geschehen erkennbar ist, dafür aber das individuelle Verhalten einer Person bereits die konkrete Wahrscheinlichkeit begründet, dass sie solche Straftaten in überschaubarer Zukunft begehen wird (BVerfG a. a. O. = BVerfGE 141, 220 [272 f.] Rn. 112; vgl. auch BayVerfGH, Entscheidung v. 13. März 2025, Vf. 5-VIII-18 pp. = BeckRS 2025, 4100 Rn. 184-187).

Allerdings ist dem Gesetzgeber – wie das BVerfG in seiner Entscheidung zum Sicherheits- und Ordnungsgesetz Mecklenburg-Vorpommerns vom 9. Dezember 2022 (1 BvR 1345/21) klargestellt hat – eine Grenze dabei gesetzt, an welche Straftaten er anknüpft. Problematisch sind hier sogenannte Vorfeldtatbestände, bei denen die Strafbarkeitsschwelle durch die Einbeziehung von Vorbereitungshandlungen in das Vorfeld von Gefahren für Rechtsgüter verlagert wird (vgl. BVerfGE 165, 1 [51] Rn. 92). Dies aber dürfte in Bezug auf die in der aktuellen Fassung des § 185a Absatz 1 Satz 2 LVwG genannten §§ 89a und 89b StGB kaum zu bestreiten sein.

Um den dargestellten Anforderungen besser gerecht zu werden, knüpft § 185a Absatz 1 Satz 2 LVwG-Entwurf die Eingriffsschwelle an einen neu einzuführenden Begriff der terroristischen Straftat. Diesen Begriff definiert § 185a Absatz 1 **Satz 3** LVwG-Entwurf – in Übereinstimmung mit § 5 Absatz 1 Satz 2 des Bundeskriminalamtsgesetzes und entsprechenden Definitionen der meisten anderen Bundesländer – durch eine Bezugnahme auf die in § 129a Absatz 1 und Absatz 2 Nummer 1 bis 3 StGB genannten Straftaten, zu denen jeweils bestimmte prägende Zielsetzungen und Gefährdungsmomente hinzutreten müssen. Diese sind wiederum im Wesentlichen durch die Richtlinie (EU) 2017/541 des Europäischen Parlaments und des Rates vom 15. März 2017 zur Terrorismusbekämpfung pp. (ABl. L 88, S. 6) vorgegeben. Von der Bezugnahme auf § 129a Absatz 2 StGB ausgenommen bleiben allerdings die in § 129a Absatz 2 Nummer 4 und 5 StGB genannten Straftatbestände des Kriegswaffenkontrollgesetzes und des Waffengesetzes. Denn diese Straftatbestände erfassen den Umgang mit Waffen und Kampfstoffen (wie das Herstellen, das Handeltreiben, den Erwerb et cetera) im Vor-

feld von Gefahren für Rechtsgüter. Demgegenüber handelt es sich bei den in § 129a Absatz 1 und Absatz 2 Nummer 1 bis 3 StGB genannten Tatbeständen um Verletzungs- und Gefährdungsdelikte, die besonders wichtige Rechtsgüter im Sinne der Rechtsprechung des BVerfG schützen.

bb) Zu § 185a Absatz 2 LVwG

§ 185a Absatz 2 LVwG legt fest, welche personenbezogenen Daten zur Überwachung und Aufzeichnung der Telekommunikation unter den Voraussetzungen des § 185a Absatz 1 LVwG erhoben werden dürfen.

Dies sind zunächst gemäß § 185a Absatz 1 Satz 1 Nummer 1 LVwG die Inhalte einer Kommunikation, soweit sie Gegenstand des (technischen) Vorganges der Nachrichtenübermittlung sind, mithin in den Schutzbereich des Fernmeldegeheimnisses (Artikel 10 GG) fallen. Ferner können gemäß der durch diesen Änderungsantrag wiedereingeführten Befugnis zur Verkehrsdatenerhebung (§ 185a Absatz 1 Satz 1 Nummer 2 LVwG-Entwurf) auch die bei einem Telekommunikationsvorgang notwendigerweise anfallenden „Begleitdaten“ (vgl. § 3 Nummer 70 TKG) erhoben werden. Auf die Erlangung solcher „Begleitdaten“ der Telekommunikation zielten auch die in § 185a Absatz 1 Nummer 2 und 3 LVwG (nach Maßgabe des Änderungsantrages künftig in: § 185a Absatz 1 Nummer 3 und 4 LVwG-Entwurf) normierten Befugnisse ab, nämlich die Feststellung des Standortes eines eingeschalteten Mobilfunkendgeräts und die Feststellung der Geräte- oder Kartennummer eines Mobilfunkendgeräts. Die Besonderheit ist, dass die letztgenannten Datenerhebungen nicht notwendig durch eine Anfrage bei einem Telekommunikationsdiensteanbieter erfolgen, sondern unter den besonderen Voraussetzungen des § 185a Absatz 3 Satz 4 LVwG (nach Maßgabe des Änderungsantrages künftig in: § 185a Absatz 3 Nummer 3 LVwG-Entwurf) auch unmittelbar durch die Polizei mit technischen Mitteln erhoben werden können. Ein solches technisches Mittel ist insbesondere der sogenannte „IMSI-Catcher“. Mithin vereinigt § 185a LVwG drei Rechtsgrundlagen in einer Vorschrift, nämlich Maßnahmen zur Telekommunikationsüberwachung, zur Verkehrsdatenerhebung und zum Einsatz technischer Mittel bei Mobilfunkendgeräten.

Im Mittelpunkt der Änderungen zu § 185a Absatz 2 LVwG steht die Wiedereinführung einer Befugnis zur Erhebung von Verkehrsdaten. Zu diesem Zweck wird § 185a Absatz 2 **Satz 1 Nummer 2** LVwG-Entwurf in die Aufzählung des § 185a Absatz 2 LVwG-Entwurf eingefügt. Die Polizei erhält damit die Möglichkeit, zu betrieblichen und vertraglichen Zwecken gespeicherte Verkehrsdaten zu erheben. Es handelt sich dabei um Daten, deren Erhebung, Verarbeitung oder Nutzung bei der Erbringung eines Telekommunikationsdienstes erforderlich sind (§ 3 Nummer 70 TKG). Als Verkehrsdaten können auch Standortdaten im Sinne

von § 3 Nummer 56 TKG anfallen, also Daten, die in einem Telekommunikationsnetz oder von einem Telekommunikationsdienst verarbeitet werden und die den Standort des Endgeräts eines Nutzers eines öffentlich zugänglichen Telekommunikationsdienstes angeben.

Die an Telekommunikationsunternehmen gerichtete Abfragebefugnis des § 185a Absatz 2 Nummer 2 LVwG-Entwurf bezieht sich nicht auf Daten, die diese Unternehmen aufgrund einer gesetzlichen Speicherpflicht vorhalten müssen (sogenannte „Vorratsdatenspeicherung“). Vielmehr können nur Verkehrsdaten abgefragt werden, die von Telekommunikationsunternehmen zu bestimmten Zwecken gemäß § 9 Absatz 1 TDDDG verarbeitet werden dürfen. Dabei dürfen zur Abrechnung mit den Endnutzern und zur Entgeltberechnung durch die Unternehmen Verkehrsdaten bis zu sechs Monate nach Versendung der Rechnung gespeichert werden (§ 10 Absatz 2 Satz 2 TDDDG). Für die Abrechnung nicht benötigte Daten sind unverzüglich zu löschen (§ 10 Absatz 2 Satz 3 TDDDG). Ferner dürfen Telekommunikationsunternehmen Verkehrsdaten zur Störungsbeseitigung und zum Aufdecken von Missbrauchsfällen durch Netzbetreiber speichern (§ 12 TDDDG). In der Praxis speichern die Telekommunikationsdiensteanbieter Verkehrsdaten zu Abrechnungs- oder IT-Sicherheitszwecken innerhalb dieses gesetzlichen Rahmens allerdings in deutlich engerem zeitlichen Umfang. Die tatsächliche Speicherfrist variiert zwischen einigen Monaten und sieben Tagen je nach Gestaltung des zugrundeliegenden Vertrags. Zudem sind die längeren Speicherfristen mittlerweile überwiegend gegenstandslos, soweit Flatrate-Modelle bei Mobilfunkverträgen vorherrschend sind, bei denen Abrechnungsdaten grundsätzlich nicht benötigt und daher auch nicht gespeichert werden dürfen. Die Sieben-Tage-Frist stellt die zulässige Höchstfrist für die Speicherung von Daten zur Störungsbeseitigung und zum Aufdecken von Missbrauchsfällen durch Netzbetreiber dar (vgl. Urt. BGH, vom 13. Jan. 2011, III ZR 146/10 = ZUM-RD 2011, 151).

Der Zugriff auf Verkehrsdaten ist für die Polizei im Einzelfall von großer Bedeutung bei der Suche nach in Not befindlichen Personen. Zwar ist es de lege lata möglich, Verkehrsdaten in Echtzeit zu erheben. So kann über § 185a Absatz 2 Nummer 2 LVwG die Funkzelle mit den Geokoordinaten des Funkturms ermittelt werden, bei dem sich das eingeschaltete Mobiltelefon zuletzt eingeloggt hat. Durch den Einsatz eines IMSI-Catchers gemäß § 185a Absatz 2 Nummer 3 LVwG lässt sich ferner ein eingeschaltetes Mobiltelefon genauer orten. Ist das Mobiltelefon einer vermissten Person jedoch nicht eingeschaltet, greifen diese Instrumente ins Leere. In diesem Fall ist lediglich eine Anfrage beim Telekommunikationsdiensteanbieter zu gespeicherten zurückliegenden Verkehrs- beziehungsweise Standortdaten geeignet, einen belastbaren Anknüpfungspunkt für Suchaktionen und Zeugenbefragungen zu liefern. Relevant ist dies nach Schätzung des Landeskriminalamtes für 20 bis 25 Sachverhalte im Jahr.

Auch in anderen gewichtigen Gefahrensituationen, wie zum Beispiel in Terror- oder Amoklagen, können rückwirkende Verkehrsdaten eine wichtige Rolle spielen. Letzte Aufenthaltsorte und Kontakte verdächtiger Personen, die anhand dieser Daten ermittelt werden können, tragen wesentlich dazu bei, dass die Polizeiführerin oder der Polizeiführer in der Lage ist, auf der Basis eines möglichst umfassenden Informationsstandes vor Ort schnell zu handeln.

§ 185a Absatz 2 **Satz 1 Nummer 3** LVwG-Entwurf gestattet, die Standortdaten eines eingeschalteten „Mobilfunkendgeräts“ zu erheben. Die Vorschrift wird lediglich redaktionell angepasst, indem der bisher verwendete Begriff „Mobilfunkendeinrichtung“ sprachlich konkreter und moderner auf „Mobilfunkendgerät“ geändert wird.

Über § 185a Absatz 2 **Satz 1 Nummer 4** LVwG-Entwurf kann die Polizei nicht bekannte Telekommunikationsanschlüsse feststellen. In die Vorschrift wird klarstellend aufgenommen, dass unter einen „Telekommunikationsanschluss“ sowohl die Gerätenummer eines Mobilfunkendgerätes als auch die Kartennummer der darin verwendeten Karte fallen. Dies ist notwendig, da die steigende Verfügbarkeit von Mobilfunkendgeräten beziehungsweise -karten erlaubt, mitunter einen stetigen Wechsel zwischen verschiedenen Geräten und Karten vorzunehmen.

§ 185a **Absatz 2 Satz 2** übernimmt die bisher in § 185a Absatz 4 LVwG enthaltene Regelung, derzufolge sich Datenerhebungen auch auf zurückliegende Zeiträume erstrecken dürfen. Diese Regelung gilt – wie bereits vor der Umgestaltung von § 185a LVwG durch das LVwGPO-RÄndG – auch für Verkehrsdatenerhebungen (vgl. § 185a Absatz 2 Satz 2 LVwG a. F.). Zugleich wird durch den neu eingeführten zweiten Halbsatz ausdrücklich klargestellt, dass Daten, die aufgrund einer gesetzlichen Verpflichtung durch Anbieter von Telekommunikationsdiensten für bestimmte Zeiträume gespeichert werden müssen, nicht als Verkehrsdaten auf Grundlage von § 185a LVwG-Entwurf erhoben werden können. Zwar ist § 175 Absatz 1 Satz 1 TKG in Verbindung mit § 176 TKG, der eine solcher Speicherverpflichtung regelt, durch Entscheidung des Bundesverwaltungsgerichts (BVerwG) mit europäischen Recht unvereinbar und daher für unanwendbar erklärt worden (siehe BVerwG, Urt. v. 14. Aug. 2023, 6 C 6.22 = NJW 2024, 98). Jedoch sieht ein aktueller Entwurf eines Gesetzes zur Einführung einer IP-Adressspeicherung und Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren (BR-Drs. 263/26) Vorgaben für Anbieter von Internetzugangsdiensten für eine dreimonatige Speicherung von IP-Adressen und zur Identifizierung erforderlicher weiterer Daten vor. Die Polizei kann – sollte dieser Gesetzentwurf umgesetzt werden – über die Anschlussinhaberin oder den Anschlussinhaber zu einer IP-Adresse lediglich nach § 180a Absatz 2 Satz 2 LVwG Auskunft verlangen.

cc) Zu § 185a Absatz 3 LVwG

§ 185a Absatz 3 LVwG-Entwurf schreibt für bestimmte Datenerhebungen – zusätzlich zu den Eingriffsvoraussetzungen des § 185a Absatz 1 LVwG-Entwurf – eine Subsidiaritätsprüfung als weitere Eingriffsvoraussetzung vor. Standortdatenerhebungen, Funkzellenabfragen und der Einsatz technischer Mittel sind danach nur zulässig, soweit die Erreichung des Zwecks der Datenerhebung – die Sachverhaltserforschung (§ 185a Absatz 1 Satz 1 LVwG-Entwurf) oder die Verhütung einer terroristischen Straftat (§ 185a Absatz 1 Satz 2 LVwG-Entwurf) – auf andere Weise aussichtslos oder wesentlich erschwert wäre.

Die zusätzliche Eingriffsvoraussetzung folgt aus dem erhöhten Eingriffsgewicht der in § 185a Absatz 3 **Nummer 1 bis 3** LVwG-Entwurf aufgelisteten Datenerhebungen. In Bezug auf Standortdatenerhebungen gilt dies deswegen, weil Standortdaten prinzipiell geeignet sind, Bewegungsprofile anzufertigen. Funkzellenabfragen sind Datenerhebungen, mit denen alle Mobilfunkgeräte erfasst werden, die sich zu einem bestimmten Zeitpunkt in einer definierten Funkzelle befinden. Sie sind durch eine hohe „Streubreite“ geprägt, weil auch Unbeteiligte, die zu einem gegebenen Zeitpunkt in einer Funkzelle mit ihrem Mobiltelefon aktiv waren, erfasst werden. Das Gewicht beider Verkehrsdatenerhebungen ist vergleichbar. Trotz der hohen „Streubreite“ ermöglicht die Funkzellenabfrage keine größeren Rückschlüsse, außer dass ein Anschlussinhaber oder eine Anschlussinhaberin zu einem bestimmten Zeitpunkt in einer bestimmten Funkzelle mit dem Mobilfunknetz verbunden war. Die Standortdatenabfrage hingegen kann, sofern Daten bei Abfrage vorhanden sind, Rückschlüsse auf Bewegungen erlauben. Doch steht der damit verbundenen höheren Eingriffstiefe eine sehr viel geringere Streubreite entgegen, da sich die Maßnahme unmittelbar auf die Anschlussinhaberin beziehungsweise den Anschlussinhaber bezieht.

In Bezug auf das Eingriffsgewicht ist bei der Standortdatenerhebung nicht zwischen zurückliegenden und zukünftigen Zeiträumen zu differenzieren. Da § 185a LVwG keinen Abruf sogenannter „Vorratsdaten“ ermöglicht, also Daten, die Telekommunikationsunternehmen aufgrund einer gesetzlichen Verpflichtung vorhalten, liefert der Abruf vorhandener Standortdaten in aller Regel nur wenig relevante Daten. Mit diesen Daten ist die Erstellung tiefgehender Bewegungsprofile über einen Zeitraum von mehreren Wochen nicht möglich. Demgegenüber können auch in die Zukunft gerichtet Standortdatenerhebungen dazu genutzt werden, ein sich ständig aktualisierendes Bewegungsprofil zu erstellen, soweit die Anordnungsentscheidung dies zulässt.

§ 185 Absatz 3 Nummer 3 LVwG-Entwurf stellt klar, dass die Polizei auch technische Mittel einsetzen darf, soweit sie den Standort eines aktiv geschalteten Mobilfunkendgeräts ermitteln (§ 185 Absatz 2 Satz 1 Nummer 3 LVwG-Entwurf) oder ihr nicht bekannte Telekommunikationsanschlüsse feststellen will (§ 185 Absatz 2 Satz 1 Nummer 4 LVwG-

Entwurf). Der Einsatz technischer Mittel war schon bisher gemäß § 185a Absatz 3 Satz 3 LVwG gestattet. Allerdings konnte die Vorschrift dahingehend missverstanden werden, dass dies nur zur Feststellung der Telekommunikationsanschlüsse, die der Polizei nicht bekannt sind, zulässig sei. Der Gesetzesbegründung ist demgegenüber zu entnehmen, dass die Vorschrift von vornherein dazu dienen sollte, den Einsatz des sogenannten „IMSI-Catchers“ zu ermöglichen (Drs. 16/670 S. 43). Ein „IMSI-Catcher“ kann jedoch – ebenso wie die sogenannte „stille SMS“, die als weiteres technisches Mittel in Betracht kommt (vgl. BGH, Beschl. v. 8. Feb. 2018, 3 StR 400/17 = NStZ 2018, 611) – dazu eingesetzt werden, Standortdaten eines Mobilfunkgeräts zu ermitteln. Tatsächlich ist die Standortbestimmung auf diese Weise deutlich genauer, als die Standortdaten die Telekommunikationsdiensteanbieter übermitteln können. Denn diese besagen lediglich, in welcher Funkzelle sich das Endgerät befindet.

dd) Weitere Änderungen gemäß § 185a Absatz 4 bis 6 LVwG

Die bisher in § 185a Absatz 3 Satz 1 LVwG normierte Adressatenregelung wird in § 185a **Absatz 4** LVwG verselbständigt und klarer gefasst. Insbesondere wird in § 185a Absatz 4 Satz 1 Nummer 2 LVwG-Entwurf künftig unzweifelhaft zum Ausdruck gebracht, dass die Datenerhebung auch zum Schutz von Personen möglich ist, die vermisst oder suizidgefährdet sind oder sich in einer hilflosen Lage befinden und die Bestimmung des Aufenthalts ansonsten aussichtslos oder wesentlich erschwert wäre. § 185a Absatz 4 Satz 2 LVwG stellt klar, dass verdeckte Überwachungsmaßnahmen zur Abwehr hinreichend konkretisierter Gefahren nur gegen die Person gerechtfertigt und auf sie nach Möglichkeit zu beschränken sind, der die Gefahr zuzurechnen ist (vgl. BVerfG, Urt. v. 20. Apr. 2016, 1 BvR 966/09 pp. = BVerfGE 141, 220 [272] Rn. 112; BVerfG Beschl. v. 9. Dez. 2022, 1 BvR 1345/21 = BVerfGE 165, 1 [50 f.] Rn. 91).

§ 185a **Absatz 5** Satz 1 und 2 LVwG-Entwurf übernimmt den Regelungsgehalt des bisherigen § 185a Absatz 3 Satz 2 und 3 LVwG mit geringfügigen redaktionellen Anpassungen. In § 185a Absatz 4 Satz 3 LVwG-Entwurf wird eine Verwendungsregelung zum Umgang mit Dritttdaten aufgenommen, soweit sie bei Funkzellenanfragen und dem Einsatz technischer Mittel anfallen können. Diese dürfen nur streng zweckgebunden für einen Datenabgleich zur Ermittlung einer gesuchten Geräte- und Kartennummer verwendet werden und sind nach Beendigung der Maßnahme unverzüglich zu löschen.

§ 185a **Absatz 6** LVwG-Entwurf führt den Regelungsgehalt des bisherigen § 185a Absatz 5 LVwG fort. Die Vorschrift erfährt allerdings eine Ergänzung hinsichtlich des Verpflichtetenkreises. Zur Ermöglichung der Überwachung und Aufzeichnung der Telekommunikation sowie zur Er-

teilung der hierfür erforderlichen Auskünfte sollen nicht nur Anbieter von Telekommunikationsdiensten (§ 3 Nummer 1 TKG) verpflichtet sein, sondern auch Stellen, die an der Erbringung von Telekommunikationsdiensten mitwirken und aufgrund ihrer tatsächlichen technischen Einbindung die Durchführung der Maßnahme ermöglichen oder die hierfür erforderlichen Auskünfte erteilen können. Damit wird klargestellt, dass die Durchführung der Maßnahme nicht dadurch erschwert oder ausgeschlossen wird, dass Telekommunikationsdienste arbeitsteilig unter Einbindung weiterer technischer Stellen, die aufgrund ihrer tatsächlichen technischen Einbindung die Überwachung und Aufzeichnung der Telekommunikation ermöglichen oder die hierfür erforderlichen Auskünfte erteilen können. Erfasst werden nur Stellen, die aufgrund ihrer tatsächlichen technischen Einbindung die Überwachung und Aufzeichnung der Telekommunikation ermöglichen oder die hierfür erforderlichen Auskünfte erteilen können. Nicht ausreichend ist hingegen eine lediglich mittelbare, rein wirtschaftliche oder unterstützende Beteiligung ohne tatsächliche Einwirkungs- oder Zugriffsmöglichkeit auf die Durchführung der Maßnahme oder die hierfür erforderlichen Daten.

c) Änderung des § 185b Absatz 1 Satz 1 LVwG

§ 185b LVwG regelt die Befugnis der Polizei, Telekommunikationsverbindungen zu unterbrechen, zu verhindern oder die Verfügungsgewalt über sie in anderer geeigneter Weise zu entziehen, unter denselben Voraussetzungen, unter denen gemäß § 185a LVwG eine Überwachung der Telekommunikation zulässig ist. Die Identität der Eingriffsschwellen von § 185a LVwG und § 185b LVwG soll erhalten bleiben, jedoch wird eine Wiederholung des Eingriffstatbestandes bei § 185b LVwG vermieden, indem die Vorschrift künftig auf § 185a verweist.

d) Änderung des § 185c LVwG

§ 185c LVwG regelt die Befugnis der Polizei, personenbezogene Daten durch die Verwendung von Vertrauenspersonen verdeckt zu erheben.

aa) Änderung von § 185c Absatz 1 Satz 2 LVwG

Die Eingriffsvoraussetzungen für eine Datenerhebung durch Verwendung von Vertrauenspersonen (§ 185c Absatz 1 Satz 2 LVwG) entsprechen bereits bisher denen des § 185 Absatz 2 LVwG. Dieser systematische Zusammenhang wird auch nach Neugestaltung des § 185 Absatz 2 LVwG – zukünftig allerdings durch eine Verweisung, statt wie bisher

durch Wiederholung der Eingriffsvoraussetzungen – fortgeführt. Er ist in der Sache gerechtfertigt. Denn der Einsatz von Vertrauenspersonen stellt eine eingriffsintensive verdeckte Maßnahme dar, die (unter bestimmten, im Rahmen von § 185c LVwG erfüllten Voraussetzungen) bei Vorliegen einer hinreichend konkretisierten Gefahr für besonders gewichtige Rechtsgüter gerechtfertigt ist (vgl. dazu BVerfG, Beschl. 9. Dez. 2022, 1 BvR 1345/21 = BVerfGE 165, 1 [48 f.] Rn. 88).

bb) Änderung von § 185c Absatz 3 und 4 LVwG

In die Tatbestände, die die Verwendung bestimmter Personen als Vertrauenspersonen ausschließen (§ 185c Absatz 3 LVwG) beziehungsweise die eine der Verwendung von Vertrauenspersonen zu bestimmten Datenerhebungen untersagen (§ 185c Absatz 4 LVwG), wird jeweils ein neuer Tatbestand aufgenommen.

e) Einführung von § 185d und § 185e LVwG-Entwurf

aa) Einführung eines § 185d LVwG-Entwurf

§ 213a LVwG-Entwurf sieht physische und technische Maßnahmen gegen unbemannte Fahrzeugsysteme vor, von denen eine Gefahr für die öffentliche Sicherheit ausgeht. Flankierend kann es zur Gefahrenabwehr in diesen Fällen erforderlich sein, personenbezogene Daten zu erheben und weiterzuverarbeiten. Dementsprechend gestattet § 185d **Absatz 1** LVwG-Entwurf, die einem unbemannten Fahrzeugsystem zuzuordnenden personenbezogenen Daten zu erheben und zu verarbeiten, insbesondere mit dem Ziel, die für den Betrieb und die Steuerung verantwortlichen Personen zu identifizieren, den Startplatz des Fahrzeugsystems zu ermitteln, den Streckenverlauf zu verfolgen und den Standort des Fahrzeugsteuerers festzustellen.

Mit umfasst sind von § 185d Absatz 1 LVwG-Entwurf namentlich Maßnahmen zur Verifikation eines detektierten Fahrzeugsystems, soweit dabei personenbezogene Daten erhoben und verarbeitet werden. Relevant ist hier in besonderem Maße die Kennung zur Fernidentifizierung von unbemannten Fluggeräten, die unter anderem die (Fern-)Identifizierung des Betreibers und Piloten, seines Standorts und eine Feststellung der Flugroute ermöglichen kann.

Der diesbezügliche rechtliche Rahmen wird insbesondere durch Vorschriften der Europäischen Union gebildet, namentlich durch die Verordnung (EU) 2018/1139 vom 4. Juli 2018 (ABl. L 212, S. 1) sowie durch die Durchführungsverordnung (EU) 2019/947 vom 24. Mai 2019 (ABl. L 152, S. 45) und die Delegierte Verordnung (EU) 2019/945 vom 12. März 2019 (ABl. L 152, S. 1). Auf diesen Vorschriften aufbauend treffen nationale Vorschriften vor allem des Luftverkehrsgesetzes (LuftVG) und in der Luftverkehrs-Ordnung weitere Regelungen.

Betreiber von (in Abhängigkeit der Betriebskategorie) zulassungspflichtigen Drohnen müssen sich gemäß § 66a Absatz 3 LuftVG beim Luftfahrt-Bundesamt mit ihren persönlichen Daten registrieren lassen. Das Luftfahrt-Bundesamt übermittelt gemäß § 66a Absatz 5 LuftVG jedem Betreiber eine Registrierungsnummer, die für alle von ihm betriebenen unbemannten Fluggeräte gilt und dem Luftfahrt-Bundesamt eine individuelle Identifizierung des Betreibers ermöglicht. Seitens des Luftfahrt-Bundesamtes wird ein persönliches Betreiberkonto mit den für die Anmeldung erforderlichen persönlichen Daten angelegt.

Insbesondere auf der Grundlage der Delegierten Verordnung (EU) 2019/945 müssen bestimmte Arten unbemannter Fluggeräte, in Abhängigkeit von der Gewichtsklasse und der Ausstattung mit Sensorsystemen zur Erfassung von personenbezogenen Daten, mit einer (direkten) Fernidentifizierung ausgestattet sein. Dabei handelt es sich um ein System, das die lokale Übertragung von Informationen über eine in Betrieb befindliche Drohne gewährleistet und auch die Kennzeichnung der Drohne umfasst, sodass diese Informationen ohne physischen Zugang zur Drohne abgerufen werden können. Zu diesen Informationen gehören Angaben über die für den Betrieb und die Steuerung jeweils verantwortliche Person, den Startplatz des unbemannten Fahrzeugsystems, den Streckenverlauf sowie den Standort des Fahrzeugsteuerers beziehungsweise den Startpunkt. Die Erhebung der mit der Fernidentifizierung verbundenen Daten ist mit technischen Mitteln möglich, beispielsweise über spezielle Apps auf Mobilfunkgeräten. Die zunächst nicht personalisierten Informationen können durch die Polizei, bei Vorliegen der rechtlichen Voraussetzungen, mit dem betreffenden Datenbestand des Luftfahrt-Bundesamtes als Registrierungsbehörde abgeglichen werden. § 185d Absatz 1 LVwG schafft die hierfür erforderliche Abfragebefugnis für die Polizei. Das Luftfahrt-Bundesamt ist auf Grundlage von § 66a Absatz 6 Nummer 4 LuftVG ermächtigt, diese Daten der abfragenden Behörde zu übermitteln.

§ 185d **Absatz 2 Satz 1** LVwG-Entwurf normiert eine Befugnis, vom Fahrzeugsteuerer eines unbemannten Fahrzeugsystems, zum Beispiel von dem Drohnenpiloten, Bildaufnahmen oder -aufzeichnungen anzufertigen, um insbesondere dessen Standort und seine Identität zu ermitteln. Das ist insbesondere von Bedeutung, wenn die Fernidentifizierung des Fluggeräts nicht aktiviert ist. Da unmittelbare Personenkontrollen durch große Distanzen erschwert sind, stellen entsprechende Aufnah-

men und Aufzeichnungen – vor allem unter Einsatz von polizeilichen Drohnen (vgl. § 185e Absatz 1 Nummer 4 LVwG-Entwurf) – ein geeignetes Mittel zur Sachverhaltsaufklärung dar. § 185d **Absatz 2 Satz 2** LVwG-Entwurf gestattet die Bildaufnahmen und -aufzeichnungen auch, soweit Dritte unvermeidbar betroffen sind.

Gemäß § 185d **Absatz 2 Satz 3** LVwG-Entwurf ist für die Speicherung und Weiterverarbeitung der Bildaufnahmen und -aufzeichnungen die Vorschrift des § 184 Absatz 6 LVwG über die Datenerhebung bei öffentlichen Veranstaltungen und Ansammlungen sowie an allgemein zugänglichen Orten anzuwenden. Danach ergibt sich eine Höchstspeicherfrist von einem Monat, falls die Daten nicht nach § 185 Absatz 2 Satz 3 in Verbindung mit § 184 Absatz 6 Satz 2 LVwG zweckändernd weiterverarbeitet werden.

§ 185d **Absatz 2 Satz 4** LVwG-Entwurf stellt klar, dass neben den nicht offenen Bildaufnahmen oder -aufzeichnungen eingriffsintensivere verdeckte Datenerhebungen gemäß § 185 LVwG, soweit erforderlich, nach Maßgabe dieser Vorschrift durchgeführt werden können.

bb) Einführung eines § 185e LVwG-Entwurf

Technische Weiterentwicklungen eröffnen die Möglichkeiten, Mittel zur Datenerhebung (Foto-, Video- und Audiotechnik) auf mobilen (unbemannten) Sensorträgern zu installieren und einzusetzen. Abhängig von dem konkreten Einsatzszenario können sich auf diese Weise signifikante operativ-taktische Mehrwerte für die Polizei ergeben. Hauptanwendungsfall eines mobilen Sensorträgers ist derzeit der Einsatz von unbemannten Fluggeräten (sogenannten Drohnen). Mobile Sensorträger können aber ebenso ein straßengebundenes Gerät oder ein (Unter-)Wasserfahrzeug sein.

§ 185e LVwG-Entwurf schafft eine neue Rechtsgrundlage für diese teilweise bereits heute genutzte Technik. Die Datenerhebung mittels mobiler, mit einem Sensorträgersystem gekoppelter Foto-, Video- und Audiotechnik findet grundsätzlich eine ausreichende Rechtsgrundlage bereits in der jeweiligen technikoffenen Ermächtigung zur Datenerhebung selbst (vgl. VG Freiburg, Urt. v. 29. Juli 2021, 10 K 4722/19, Rn. 63 f. = MMR 2021, 1013 [1017] in Bezug auf Übersichtsaufnahmen bei Versammlungen). § 185e LVwG-Entwurf schafft jedoch dafür Rechtssicherheit und einen klaren Handlungsrahmen. Die Verankerung der Nutzung von mobilen Sensorträgersystemen durch die Polizei im LVwG ist auch deswegen von großer Bedeutung, weil der Einsatz von polizeilichen Drohnen zur Drohnenabwehr unerlässlich ist.

Vor diesem Hintergrund stellt § 185e **Absatz 1 Satz 1** LVwG-Entwurf klar, dass eine nach anderen Vorschriften zulässige Datenerhebung auch durch den Einsatz mobiler Sensorträger erfolgen kann. Die Vorschrift ermächtigt mithin nicht zur Erhebung personenbezogener Daten. Vielmehr setzt sie voraus, dass die Tatbestandsvoraussetzungen zur Erhebung personenbezogener Daten durch offenen oder verdeckten Einsatz technischer Mittel nach einer der in dieser Norm aufgeführten Ermächtigungsgrundlagen erfüllt sind. § 185e **Absatz 1 Satz 2** LVwG-Entwurf zählt die in Betracht kommenden Bezugsnormen zur Datenerhebung abschließend auf, nämlich:

- § 184 Absatz 1 bis 5 LVwG: Datenerhebung bei öffentlichen Veranstaltungen und Ansammlungen sowie an allgemein zugänglichen Orten;

- § 185 Absatz 1 Nummer 1 und 2 LVwG: Observation und verdeckter Einsatz technischer Mittel zur Datenerhebung;

- § 185 Absatz 3 LVwG: Einsatz technischer Mittel zur Datenerhebung in oder aus Wohnungen;

- § 185a LVwG: Telekommunikationsüberwachung;

- § 185d LVwG-Entwurf: Datenerhebung im Zusammenhang mit der Abwehr unbemannter Fahrzeugsysteme.

§ 185e **Absatz 2** LVwG-Entwurf stellt klar, dass offene Datenerhebungen gemäß § 184 Absatz 1 bis 5 LVwG auch beim Einsatz mobiler Sensorträgersysteme offen durchgeführt werden müssen. Um die Offenheit zu wahren, soll ein gesonderter Hinweis auf die Datenerhebung durch Sensorträgersysteme erfolgen, beispielsweise, dass Drohnen zur Erhebung von Daten genutzt werden. Dies kann auf unterschiedliche Art und Weise geschehen. So kommt in Betracht, dass der Einsatzort entsprechend beschildert wird, aber auch, dass die Drohne oder die Person, die sie steuert, eine besondere, auffällige Markierung trägt. Von dem Hinweis kann ausnahmsweise abgesehen werden, wenn seine Umsetzung aufgrund besonderer Umstände des Einzelfalles (zum Beispiel einer besonderen Dringlichkeit) nicht möglich ist, und der Verzicht auf den Hinweis im Verhältnis zur abzuwehrenden Gefahrenlage respektive den abzuwendenden Schäden gerechtfertigt erscheint.

§ 185e **Absatz 3** schreibt vor, dass dann, wenn ein unbemanntes Fahrzeugsystem (zum Beispiel eine Drohne) als Sensorträgersystem zur Datenerhebung genutzt wird, dieses nicht mit Mitteln des unmittelbaren Zwangs gemäß § 251 Absatz 3 und 4 LVwG ausgestattet sein darf. Eine Ausnahme bildet allein der Fall, in dem das unbemannte Fahrzeugsystem der Polizei in Verbindung mit einer Maßnahme zur Abwehr

von unbemannten Fahrzeugsystemen nach § 213a LVwG-Entwurf eingesetzt wird.

f) Änderung des § 186 LVwG

§ 186 wird nur geringfügig redaktionell ergänzt. § 186 Absatz 1 Nummer 6 LVwG-Entwurf wird an die neue Überschrift des § 185a LVwG und der Verweis in § 186 Absatz 7 LVwG an die Neuordnung des § 185a LVwG angepasst.

g) Änderung des § 186a LVwG

§ 186a Absatz 1 bis 5 LVwG bündelt die besonderen Schutzmechanismen für den **Kernbereich privater Lebensgestaltung** bei Maßnahmen nach §§ 185, 185a und § 185c LVwG. Die mit dem LVwGPORÄndG vom 26. Februar 2021 eingeführten Regelungen sind in Ansehung der Entscheidung des BVerfG zum Sicherheits- und Ordnungsgesetz Mecklenburg-Vorpommerns vom 9. Dezember 2022 (1 BvR 1345/21 / BVerfGE 165, 1 [56 ff.] Rn. 100 ff.) – gerade in Bezug auf den Einsatz von Vertrauenspersonen (VP) und verdeckt ermittelnden Personen (VE) – zu reformieren.

Die Neuregelung trägt den unterschiedlichen Erscheinungsformen verdeckter Datenerhebung Rechnung. Das BVerfG betont, dass neben heimlichen Überwachungsmaßnahmen insbesondere auch der Einsatz von VP und VE typischerweise zur Erhebung kernbereichsrelevanter Daten führen kann. Es stellt zugleich klar, dass hierbei bereits die Art und Weise der verdeckten Datenerhebung, insbesondere die Interaktion zwischen der eingesetzten Person und der Zielperson, den Kernbereich privater Lebensgestaltung berühren kann, ohne dass es auf den Inhalt der erlangten Information ankommt. Dies gilt namentlich dann, wenn ein Vertrauensverhältnis aufgebaut oder ausgenutzt wird, das den engsten persönlichen Bindungen entspricht. Dem trägt die Vorschrift Rechnung, indem sie den Kernbereichsschutz nicht nur inhaltlich, sondern auch hinsichtlich der Modalitäten der Datenerhebung absichert und den Schutz bereits auf der Ebene der Einsatzplanung, der laufenden Durchführung und der Auswertung anordnet.

Insgesamt folgt die Regelung einem mehrstufigen Schutzkonzept: Zunächst sind Maßnahmen unzulässig, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass durch sie allein Daten aus dem Kernbereich privater Lebensgestaltung erlangt werden oder bereits die Art und Weise ihrer Durchführung in den Kernbereich eingreift. Ergeben sich während der laufenden Maßnahme tatsächliche Anhaltspunkte für eine Kernbereichsbetroffenheit, ist die Maßnahme unverzüglich zu unterbrechen oder, soweit ausreichend, zu beschränken. Für personengebundene verdeckte Datenerhebungen werden besondere Aufschubregelungen geschaffen, die der Eigenart dieser Maßnahmen Rechnung tragen. Bei Zweifeln über die Betroffenheit des Kernbereichs sieht die Vor-

schrift für bestimmte technisch geprägte Maßnahmen eine Fortsetzung im Wege der automatischen Aufzeichnung vor. Kernbereichssensible Daten unterliegen zudem einer besonderen gerichtlichen Kontrolle, bevor sie verwertet werden dürfen.

aa) Zur Änderung der Überschrift des § 186a LVwG

Die Überschrift wird redaktionell angepasst.

bb) Zur Änderung von § 186a Absätze 1 bis 4 LVwG

§ 186a **Absatz 1 Satz 1** LVwG bestimmt, dass Maßnahmen nach §§ 185, 185a und § 185c LVwG unzulässig sind, wenn tatsächliche Anhaltspunkte dafür vorliegen, dass durch sie allein Daten aus dem Kernbereich privater Lebensgestaltung erlangt werden, oder bereits die Art und Weise ihrer Durchführung in den Kernbereich eingreift.

Damit wird zum einen klargestellt, dass sich der Kernbereichsschutz nicht nur auf den möglichen Inhalt der erhobenen Daten bezieht, sondern auch auf die Modalitäten der Maßnahme selbst. Mit der Entscheidung zum Sicherheits- und Ordnungsgesetz Mecklenburg-Vorpommerns hat das BVerfG (erstmals) klargestellt, dass bei personengebundenen verdeckten Maßnahmen ein Eingriff in den Kernbereich auch durch die Art der Interaktion, etwa beim Aufbau oder der Nutzung eines persönlichen Vertrauensverhältnisses, das engsten persönlichen Bindungen entspricht, erfolgen kann (BVerfG, Beschl. v. 9. Dez. 2022, 1 BvR 1345/21 = BVerfGE 165, 1 [57, 59] Rn. 103, 107).

Bereits vorab ist zu prüfen, ob Anhaltspunkte dafür bestehen, dass der geplante Einsatz kernbereichsrelevante Informationen erfassen wird (BVerfG, Beschl. v. 9. Dez. 2022, 1 BvR 1345/21 = BVerfGE 165, 1 [61 f.] Rn. 111 f.). Soweit Äußerungen, Handlungen oder Interaktionen unmittelbar selbst strafbares Verhalten darstellen oder der Begehung, Verabredung oder Durchführung von Straftaten zuzuordnen sind, fallen sie nicht in den Schutzbereich des Kernbereichs privater Lebensgestaltung (BVerfG, Urt. v. 3. März 2004, 1 BvR 2378/98 pp. = BVerfGE 109, 279 [319] Rn. 137; BVerfG, Urt. v. 20. April 2016, 1 BvR 966/09 pp = BVerfGE 141, 220 [277] Rn. 122). Dies ist insbesondere in sensiblen Bereichen verdeckter Ermittlungen von Bedeutung, in denen szenetypisches Verhalten den bewussten Umgang mit derartig strafrechtlich relevanten Inhalten voraussetzt. Dies ist erfasst zum Beispiel Ermittlungen in Foren, die mit Missbrauchsdarstellungen umgehen, oder die Kommunikation in Bezug auf ein Sexualdelikt. Auch soweit einzelne Inhalte wegen ihres unmittelbaren Bezugs zu Straftaten nicht dem Kernbereichs-

schutz unterfallen, bleibt maßgeblich, dass die Art und Weise der Datenerhebung nicht selbst kernbereichsrelevant ausgestaltet sein darf.

Vor diesem Hintergrund verpflichtet § 186a **Absatz 1 Satz 2** LVwG vor Durchführung der Maßnahmen sowohl zu technischen Vorkehrungen als auch zu organisatorischen Maßnahmen, um Verletzungen des Kernbereichs privater Lebensgestaltung zu vermeiden. Damit wird hervorgehoben, dass der Schutz des Kernbereichs nicht einseitig technisch oder ausschließlich organisatorisch gewährleistet werden kann, sondern je nach Art der Datenerhebung unterschiedliche Schutzanforderungen bestehen. Bei technisch geprägten Maßnahmen können vorrangig technische Schutzvorkehrungen in Betracht kommen; bei personengebundenen verdeckten Datenerhebungen werden regelmäßig organisatorische Maßnahmen, insbesondere Auswahl, Schulung, Belehrung und einsatzbezogene Sensibilisierung der eingesetzten Personen, von besonderem Gewicht sein. Von geeigneten Vorkehrungen und Maßnahmen darf nur abgesehen werden, wenn sie trotz des Gewichts des Eingriffs mit unverhältnismäßigem Aufwand verbunden wären.

§ 186a **Absatz 2** LVwG regelt die Rechtsfolgen, wenn sich während einer laufenden Maßnahme tatsächliche Anhaltspunkte dafür ergeben, dass Inhalte aus dem Kernbereich privater Lebensgestaltung erfasst werden oder die Art und Weise der Durchführung in den Kernbereich eingreift. In diesen Fällen ist die Maßnahme gemäß § 186a **Absatz 2 Satz 1** LVwG unverzüglich zu unterbrechen oder, soweit dies zur Vermeidung eines weiteren Eindringens in den Kernbereich ausreicht, zu beschränken. Damit greift die Vorschrift die Vorgabe des BVerfG auf, schon auf der Ebene der Datenerhebung den Abbruch der Maßnahme vorzusehen, wenn erkennbar wird, dass eine Überwachung in den Kernbereich privater Lebensgestaltung eindringt (im Einzelnen: BVerfG, Beschl. v. 9. Dez. 2022, 1 BvR 1345/21, = BVerfGE 165, 1 [60 ff.] Rn. 110 ff.). Die Möglichkeit der Beschränkung trägt dem Umstand Rechnung, dass nicht in jedem Fall nur ein vollständiger Abbruch geeignet ist, ein weiteres Eindringen in den Kernbereich zu verhindern.

Für den Einsatz von Personen zur verdeckten Datenerhebung nach § 185 Absatz 1 Nummer 3 und § 185c LVwG werden in § 186a **Absatz 2 Satz 2 und 3** LVwG besondere Aufschubregelungen geschaffen. Damit wird der Eigenart personengebundener Maßnahmen Rechnung getragen. Das BVerfG weist darauf hin, dass die Zielperson Verdacht schöpfen kann, wenn eine Datenerhebung wegen des Eindringens in den Kernbereich vor Ort und unvermittelt abgebrochen werden muss; ein sofortiger Abbruch kann dadurch zu einer Enttarnung führen und damit zugleich eine erhebliche Gefahr für Leib und Leben der eingesetzten Person begründen (BVerfG, Beschl. v. 9. Dez. 2022, 1 BvR 1345/21 = BVerfGE 165, 1 [62 f.] Rn. 114). Vor diesem Hintergrund kann eine Ausnahme vom Abbruchgebot verfassungsrechtlich gerechtfertigt sein, wenn andernfalls Leib oder Leben der VP oder VE in Gefahr gerieten (BVerfG, Beschl. v. 9. Dez. 2022, 1 BvR 1345/21 = BVerfGE

165, 1 [63 f.] Rn. 115 f.). Satz 2 beschränkt den Aufschub deshalb auf diesen eng umgrenzten Fall. Andere drohende Nachteile oder Einbußen an sonstigen Rechtsgütern rechtfertigen einen Aufschub demgegenüber nicht. Satz 3 eröffnet daneben einen eigenständigen, ebenfalls eng begrenzten Ausnahmefall. Das BVerfG erkennt insoweit auch das ermittlungstechnische Bedürfnis an, den weiteren Einsatz einer VP und VE zu sichern (BVerfG, Beschl. v. 9. Dez. 2022, 1 BvR 1345/21 = BVerfGE 165, 1 [63 f.] Rn. 115 f.). Danach kommt ein Aufschub aber nur in Betracht, wenn konkret dargelegt werden kann, dass die weitere Verwendung der eingesetzten Person gefährdet wäre.

§ 186a **Absatz 2 Satz 4** LVwG erlaubt bei bestimmten technisch geprägten Maßnahmen im Fall fortbestehender Zweifel über die Betroffenheit des Kernbereichs eine Fortsetzung der Maßnahme im Wege der automatischen Aufzeichnung. Die automatische Aufzeichnung dient dazu, eine inhaltliche Kenntnisnahme durch die Polizei zunächst zu verhindern und die weitere Prüfung einer nachgelagerten Kontrolle zuzuführen.

§ 186a **Absatz 2 Satz 5** LVwG stellt klar, dass nach einem Abbruch oder einer Beschränkung die Maßnahme und die Art und Weise ihrer Durchführung erneut zu bewerten sind. Eine Fortsetzung ist nur zulässig, wenn aufgrund tatsächlicher Anhaltspunkte anzunehmen ist, dass kernbereichsrelevante Erkenntnisse nicht erfasst werden.

§ 186a **Absatz 3** LVwG regelt die gerichtliche Kontrolle besonders kernbereichssensibler Daten. Daten, die durch Maßnahmen nach § 185 Absatz 3 LVwG erhoben wurden, sind dem zuständigen Gericht unverzüglich vorzulegen. Gleiches gilt für Daten, die im Wege der automatischen Aufzeichnung nach § 186a Absatz 2 Satz 4 LVwG erhoben wurden. Das Gericht entscheidet unverzüglich über die Verwertbarkeit oder Löschung der Daten. Damit wird sichergestellt, dass bei Maßnahmen mit besonderer Kernbereichsnähe sowie in Fällen fortbestehender Zweifel an der Betroffenheit des Kernbereichs eine unabhängige gerichtliche Kontrolle vor einer polizeilichen Verwertung stattfindet. Für den bislang nicht ausdrücklich geregelten Fall, dass eine automatische Aufzeichnung nach § 186a Absatz 2 Satz 4 LVwG im Rahmen einer Maßnahme erfolgt, der keine gerichtliche Anordnung vorausgegangen ist, bestimmt die Vorschrift das nach § 186 Absatz 6 Satz 1 LVwG zuständige Gericht als zuständig.

§ 186a **Absatz 4** LVwG enthält eine Gefahr-im-Verzug-Regelung für die vorläufige Entscheidung über die Verwertung in Fällen des § 186a Absatzes 3 LVwG. Kann das Gericht nicht rechtzeitig erreicht werden, darf die Entscheidung vorläufig durch die Leitungsebene der genannten Polizeibehörden oder eine durch die jeweilige Leitungsebene besonders beauftragte Person im Benehmen mit der oder dem behördlichen Datenschutzbeauftragten getroffen werden. Die gerichtliche Entscheidung ist unverzüglich nachzuholen. Die Regelung trägt dem Bedürfnis Rech-

nung, in zeitkritischen Konstellationen handlungsfähig zu bleiben, ohne auf die gebotene richterliche Kontrolle zu verzichten. Zugleich setzt sie die Vorgabe der Rechtsprechung um, dass bei Zweifeln an der Kernbereichsrelevanz eine unabhängige Stelle einzubinden ist (siehe: Begründung zur Einführung eines § 186a Absatz 4a LVwG). Mit dem Erfordernis des Benehmens mit der oder dem behördlichen Datenschutzbeauftragten wird dieser Mindestanforderung auch für die vorläufige Entscheidung im Eilfall Rechnung getragen.

cc) Zur Einführung eines § 186a Absatzes 4a LVwG-Entwurf

§ 186a **Absatz 4a** LVwG setzt die vom BVerfG hervorgehobene Vorgabe um, dass auf der Ebene der nachgelagerten Auswertung und Verwertung die Folgen eines dennoch erfolgten Eindringens in den Kernbereich privater Lebensgestaltung strikt zu minimieren sind. Die bisherigen Vorkehrungen des geltenden Rechts reichen insoweit nicht aus und werden durch die Neuregelung ergänzt. Die Vorschrift betrifft nicht die spontane Steuerung der Maßnahme vor Ort, sondern die Phase nach Erlangung der Information.

§ 186a **Absatz 4a Satz 1** LVwG ordnet als Grundsatz an, dass die Weiterverarbeitung unverzüglich zu unterbleiben hat, wenn sich bei der Auswertung ergibt, dass Daten Inhalte aus dem Kernbereich privater Lebensgestaltung betreffen oder bereits durch die Art und Weise der Durchführung in den Kernbereich eingegriffen wurde. Darüber hinaus stehen im Mittelpunkt der Vorschrift zwei vom BVerfG besonders hervorgehobene Sicherungsmechanismen.

Erstens wird für personengebundene verdeckte Datenerhebungen in § 186a **Absatz 4a Satz 2** LVwG die Pflicht normativ verankert, dass die eingesetzten Personen und insbesondere deren polizeiliche Führungspersonen erlangte Erkenntnisse vor jeder Weitergabe auf ihre Kernbereichsrelevanz zu prüfen haben. Das entspricht der Rechtsprechung des BVerfG, wonach sowohl zum einen die VP oder VE bereits vor der Weitergabe selbst zu prüfen hat, ob der Kernbereich privater Lebensgestaltung berührt ist, als auch die Führungsperson der VP oder VE die Kernbereichsrelevanz vor einer Verwertung überprüfen muss (BVerfG, Beschl. v. 9. Dez. 2022, 1 BvR 1345/21 = BVerfGE 165, 1 [64 f.] Rn. 117f.).

Zweitens wird gemäß § 186a **Absatz 4a Satz 3** LVwG für Zweifelsfälle eine zusätzliche Klärung unter Einbindung einer unabhängigen Stelle vorgesehen. Dies trägt der weiteren Vorgabe des BVerfG Rechnung, dass in Zweifelsfällen eine Klärung der Kernbereichsrelevanz zumindest durch die behördlichen Datenschutzbeauftragten zu erfolgen hat (BVerfG, Beschl. v. 9. Dez. 2022, 1 BvR 1345/21 = BVerfGE 165, 1 [65] Rn. 119). Klärungsbedürftig kann dabei insbesondere die Frage sein,

ob ein bereits erhobenes Datum wegen seines Kernbereichsbezugs zu löschen ist oder ausnahmsweise verwertbar bleibt, weil die möglicherweise kernbereichsrelevanten Informationen ihrerseits Gegenstand einer Straftat waren. Die Bewertung dieser Frage verbleibt beim Verantwortlichen. Die Formulierung „im Benehmen mit der oder dem behördlichen Datenschutzbeauftragten“ stellt zugleich klar, dass die oder der behördliche Datenschutzbeauftragte in ihrer oder seiner unabhängigen beratenden Funktion einzubinden ist, ohne dass die Verantwortlichkeit für die Entscheidung verlagert würde. Verbleiben Zweifel an der Verwertbarkeit, sind die Daten gemäß § 186a **Absatz 4a Satz 4** LVwG grundsätzlich unverzüglich zu löschen. Jedoch kann an die Stelle der Löschung eine gerichtliche Bestätigung der Verwertbarkeit auf Grundlage von § 186a **Absatz 4a Satz 5** LVwG treten. Der Entwurf ordnet damit keinen starren Erkenntnisverlust an, sondern eröffnet für Zweifelsfälle eine unabhängige gerichtliche Klärung. Die Vorschrift stellt so sicher, dass kernbereichssensible Erkenntnisse nicht ungeprüft weitergegeben oder verwertet, sondern im Zweifel gelöscht oder einer gerichtlichen Entscheidung zugeführt werden.

dd) Zur Änderung des § 186a Absatz 5 LVwG

§ 186a **Absatz 5** LVwG stellt klar, dass Daten, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, nicht verwertet werden dürfen und unverzüglich zu löschen sind. Damit wird der absolute Schutz des Kernbereichs privater Lebensgestaltung auf der Ebene der Datenverwendung abgesichert. Nach der Rechtsprechung des BVerfG gewährleistet der Kernbereich einen Bereich höchstpersönlicher Privatheit gegenüber Überwachung und sichert einen dem Staat nicht verfügbaren Menschenwürdekern grundrechtlichen Schutzes; selbst überragende Interessen der Allgemeinheit können einen Eingriff in diesen Bereich nicht rechtfertigen. Dementsprechend ordnet die Vorschrift für kernbereichsrelevante Daten ein ausnahmsloses Verwertungsverbot und ihre unverzügliche Löschung an.

ee) Zur Einführung eines § 186a Absatz 5a LVwG-Entwurf

§ 186a **Absatz 5a** LVwG normiert die Dokumentationspflichten und setzt die vom BVerfG geforderte nachträgliche Kontrollierbarkeit kernbereichsrelevanter Vorgänge um. Das BVerfG verlangt, dass in Zweifelsfällen eine Klärung der Kernbereichsrelevanz zumindest durch die behördlichen Datenschutzbeauftragten erfolgt und dass das Festgehaltene sofort gelöscht oder sonst vernichtet, jegliche Verwendung unterlassen und dies in einer Weise dokumentiert wird, die eine spätere Kontrolle ermöglicht; jedenfalls ist der Umstand zu dokumentieren, dass in den Kernbereich privater Lebensgestaltung vorgedrungen wurde

(BVerfG, Beschl. v. 9. Dez. 2022, 1 BvR 1345/21 = BVerfGE 165, 1 [65] Rn. 119). Zu dokumentieren sind deshalb

- die Tatsache der Erhebung von Daten, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, und ihre Löschung aus diesem Grund,

- die Unterbrechung oder Beschränkung einer Maßnahme einschließlich eines etwaigen Aufschubs und der Fortsetzung einer Maßnahme nach Unterbrechung oder Beschränkung einschließlich der jeweils tragenden Gründe,

- die Entscheidung über die Verwertung von Erkenntnissen bei Gefahr im Verzug nach § 186a Absatz 4 LVwG sowie

- die Durchführung einer Prüfung nach § 186a Absatz 4a Satz 3 LVwG und ihr Ergebnis.

Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist sechs Monate nach der Benachrichtigung oder der Erteilung der gerichtlichen Zustimmung zum endgültigen Absehen von der Benachrichtigung zu löschen; ist die Datenschutzkontrolle noch nicht beendet, ist die Dokumentation bis zu ihrem Abschluss aufzubewahren.

8. Zu Nummer 8 (Anpassung der Nummerierung der Drs. 20/4248)

Der Änderungsantrag bedingt eine Änderung der Nummernfolge der Änderungsbefehle der Drs. 20/4284. Die bisherigen Nummern 5, 6 und 7 werden zu Nummer 16, 17 und 18.

9. Zu Nummer 9 (Änderung von § 189 Absatz 1 Satz 4 LVwG)

In § 189 Absatz 1 Satz 4 LVwG werden die Voraussetzungen für die weitere Verarbeitung personenbezogener Daten, die im Rahmen von Strafermittlungsverfahren über eine tatverdächtige Person gewonnen wurden, neu gefasst. Die Vorschrift bleibt Regelungsgrundlage für die weitere Speicherung solcher Daten. Sie befugt die Polizei sowohl zum Führen sogenannter Kriminalakten als auch von Dokumentationen vorhandener Kriminalakten (sogenannter Kriminalaktennachweis/KAN). Bereits mit dem LVwGPORÄndG vom 26. Februar 2021 sind die Voraussetzungen hierfür geöffnet worden. Gleichwohl erscheinen sie im Ländervergleich, insbesondere im Verhältnis zu anderen norddeutschen Bundesländern, weiterhin erhöht. Die Änderung dient daher einer weiteren Annäherung an die Regelungen des Bundes und anderer Län-

der, um eine möglichst einheitliche Praxis im Bundesgebiet zu gewährleisten. Zugleich werden die normativen Vorgaben für die Prognoseentscheidung mit § 183 Absatz 1 Satz 3 LVwG abgestimmt, um eine höhere systematische Kohärenz zwischen den Vorschriften zu erreichen.

Der bisher in § 189 Absatz 1 Satz 4 LVwG aufgeführte Speicherzweck der „Aufklärung künftiger Straftaten“ entfällt. Dieser Zweck betrifft ausschließlich die Strafverfolgungsvorsorge, welche der künftigen Strafverfolgung in Bezug auf mögliche spätere oder später bekannt werdende Straftaten dient und kompetenzrechtlich dem gerichtlichen Verfahren im Sinne des Artikels 74 Absatz 1 Nummer 1 GG zugeordnet ist (BVerfG, Urt. v. 27. Juli 2005, 1 BvR 668/04 = BVerfGE 113, 348 [370]). Für die Speicherung von Daten aus Strafverfahren zu Zwecken künftiger Strafverfahren hat der Bund jedoch auf der Grundlage des genannten Kompetenztitels mit § 484 Absatz 1 bis 3 StPO eine bundesrechtliche Regelung getroffen (vgl. BVerwG, Urt. v. 25. Januar 2012, 6 C 9/11 = NVwZ 2012, 757 [760] Rn. 36). Lediglich die weitere Verarbeitung der Daten, die für Zwecke künftiger Strafverfahren von der Polizei gespeichert sind, richtet sich – wenn sie zu anderen Zwecken erfolgt, als die Nutzung der Daten für ein konkretes Strafverfahren bei Eintritt des Vorsorgefalles – nach den Polizeigesetzen der Länder. Das heißt, die auf Grundlage von § 484 Absatz 1 bis 3 StPO gespeicherten Daten werden weitgehend nach den Regelungen der Polizeigesetze behandelt werden (vgl. VGH München, Beschl. v. 3. Apr. 2013, 10 C 11.1967 = BeckRS 2013, 50639 Rn. 4; Singelstein in: MüKoStPO, 2. Aufl. 2024, StPO § 484 Rn. 21). Bis 2019 verwies § 484 Absatz 4 StPO ausschließlich in Bezug auf die „Verwendung“ der gespeicherten repressiven Daten auf die Polizeigesetze. Mit der Änderung des Wortlautes durch das Gesetz vom 20. November 2019 (BGBl. I S. 1724) sollte lediglich eine sprachliche Anpassung an die Richtlinie (EU) 2016/680, nicht jedoch eine materielle Änderung herbeigeführt werden (BT-Drs. 19/4671 S. 67). Umgekehrt folgt aus der expliziten Zuordnung nur eines Teils der Regelungsmaterie zum Landesrecht, dass § 484 StPO insgesamt als eine abschließende Regelung auf dem Gebiet der Strafverfolgungsvorsorge zu betrachten ist; folglich verbleibt kein Regelungsspielraum für das Land. Daher wird § 189 Absatz 1 Satz 4 LVwG auf den präventivpolizeilichen Zweck der Verhütung künftiger Straftaten beschränkt.

10. Zu Nummer 10 (Anpassung der Nummerierung der Drs. 20/4284)

Der Änderungsantrag bedingt eine Änderung der Nummernfolge der Änderungsbefehle der Drs. 20/4284. Die bisherigen Nummern 8, 9, 10, 11 und 12 werden zu Nummern 20, 21, 22, 23, 24 und 25.

11. Zu Nummer 11 (Änderungen von Nummer 14 der Drs. 20/4284)

a) Anpassung der Nummerierung der Drs. 20/4284

Der Änderungsantrag bedingt eine Änderung der Nummernfolge der Änderungsbefehle der Drs. 20/4284. Die bisherige Nummer 14 wird zur Nummer 26.

b) Zu Buchstaben b und c (Änderung von § 201c LVwG)

Dieser Änderungsantrag sieht eine Definition des Begriffs der „terroristischen Straftat“ in § 185a Absatz 1 Satz 3 LVwG-Entwurf vor, die identisch ist mit der Definition des § 201c Absatz 1 Satz 2 LVwG-Entwurf. Damit wird eine selbständige Begriffsbestimmung für § 201c Absatz 1 LVwG entbehrlich.

12. Zu Nummer 12 (Anpassung der Nummerierung der Drs. 20/4284)

Der Änderungsantrag bedingt eine Änderung der Nummernfolge der Änderungsbefehle der Drs. 20/4284. Die bisherige Nummer 15 wird zur Nummer 27.

13. Zu Nummer 13 (Änderung des § 202 Absatz 2 LVwG)

§ 202 Absatz 2 LVwG regelt Befugnisse der Polizei zur Durchsuchung von Personen. Die mit diesem Änderungsantrag eingebrachten Änderungen der Vorschrift haben unterschiedliche Zielrichtungen:

§ 202 Absatz 2 Nummer 2 LVwG wird klarstellend überarbeitet.

Der neu gefasste § 202 Absatz 2 Nummer 3 LVwG erweitert die Durchsuchungsbefugnis für bestimmte Kontrollsituationen.

§ 202 Absatz 2 Nummer 4 LVwG übernimmt den Regelungsgehalt des bisherigen § 202 Absatz 2 Nummer 3 LVwG, der zugleich redaktionell angepasst wird.

a) Änderung von § 202 Absatz 2 Nummer 2 LVwG

Als Reaktion auf Unsicherheiten in der Praxis wird § 202 Absatz 2 Nummer 2 LVwG neu gefasst. Die Rechtsunsicherheit besteht darin, dass die Vorschrift ihrem aktuellen Wortlaut nach die Durchsuchung in Fällen gestattet, in denen

„eine Identitätsfeststellung aufgrund des § 181 Absatz 1 Satz 2 Nummer 1 bis 4 LVwG zulässig ist“. Diese Formulierung ist geeignet, dahin missverstanden zu werden, als sei eine Durchsuchung nur dann zulässig, wenn auch eine Identitätsfeststellung durchgeführt werden kann. In Fällen, in denen die Identität einer Person bereits feststeht – also eine Identitätsfeststellung nicht durchgeführt werden soll beziehungsweise nicht erforderlich wäre –, könnte man so gesehen die Durchsuchung nicht auf § 202 Absatz 2 Nummer 2 LVwG stützen. Diese Sichtweise ist jedoch verfehlt. Eine solche Verknüpfung zwischen Identitätsfeststellung und Personendurchsuchung wäre nur dann sachgerecht, wenn die Durchsuchung gerade der Identitätsfeststellung dienen soll. Das ist jedoch offensichtlich nicht Regelungsziel von § 202 Absatz 2 Nummer 2 LVwG. Denn eine Befugnis zur Durchsuchung mit dem Ziel der Identitätsfeststellung existiert bereits in Gestalt von § 181 Absatz 4 Satz 3 LVwG. Es ist daher bei Einführung der Durchsuchungsbefugnis gemäß § 202 Absatz 2 Nummer 2 LVwG (als § 202 Absatz 1 Nummer 3 des LVwG in der Fassung von 1992, vgl. GVOBl. Schl.-H. S. 295) der erkennbare Wille des Gesetzgebers gewesen, Durchsuchungen von Personen allein unter der Voraussetzung zu gestatten, dass sich die zu durchsuchende Person an einem Ort befindet, für den die Voraussetzungen des § 181 Absatz 1 Satz 2 Nummer 1 bis 4 LVwG vorliegen (vgl. Drs. 12/1575, S. 62 unter Bezugnahme auf § 17 des Musterentwurfs eines einheitlichen Polizeigesetzes von 1976). Dies stellt der neue Wortlaut der Vorschrift eindeutig klar.

b) Neufassung von § 202 Absatz 2 Nummer 3 LVwG

§ 202 Absatz 2 Nummer 3 LVwG implementiert in Fällen, in denen gemäß § 181 Absatz 1 Satz 2 Nummer 5 LVwG die Identität einer Person festgestellt werden darf, eine ergänzende Durchsuchungsbefugnisse. Dabei geht es um Kontrollen in öffentlichen Einrichtungen des internationalen Verkehrs sowie auf Durchgangsstraßen zum Zwecke der Bekämpfung der grenzüberschreitenden Kriminalität oder von Straftaten von erheblicher Bedeutung.

Für eine Befugnis zur Durchsuchung der Person an Orten, die keine besondere Gefahrennähe aufweisen, sondern durch ein strukturell abstraktes Gefahrenpotential gekennzeichnet sind, ist verfassungsrechtlich eine Einschreitschwelle in Gestalt einer „erhöhten abstrakten Gefahr“ geboten, die über allgemeine Lageerkenntnisse oder polizeiliche Erfahrungssätze hinausgehende, zusätzliche und als solche hinreichend greifbare Erkenntnisse fordert (BayVerfGH, Entscheidung v. 7. Feb. 2006, Vf. 69-VI-04 = NVwZ 2006, 1284 [1287]). Damit ist eine gegenüber der Identitätsfeststellung erhöhte Eingriffsschwelle erforderlich (BayVerfGH a. a. O). Diese verfassungsrechtliche Vorgabe setzt der § 202 Absatz 2 Nummer 3 LVwG dadurch um, dass die Durchsuchung eine auf Tatsachen gestützte Prognose erfordert, aufgrund derer die Maßnahme zur Erreichung der von § 181 Absatz 1 Satz 2 Nummer 5 LVwG vorgegebenen Zwecke erforderlich sein muss. Voraussetzung der Durchsuchung ist demgemäß nicht nur das Antreffen der Person an einem der einschlägigen Orte. Gefordert ist darüber hinaus, dass Tatsachen die Erforderlichkeit der

Durchsuchung zur Bekämpfung der grenzüberschreitenden Kriminalität beziehungsweise zur Verhütung einer erheblichen Straftat rechtfertigen. Eine konkrete Gefahr muss dafür nicht vorliegen; vielmehr setzt die Befugnis im Vorfeld einer konkreten Gefahr an. Erforderlich sind Tatsachen, die den Schluss auf eine erhöhte abstrakte Gefahr der grenzüberschreitenden Kriminalität oder anderer bestimmter Straftaten zulassen. Dies können verdichtete Lageerkenntnisse sein, die sich in der Durchsuchungssituation manifestieren, oder Täterprofile und Fahndungsraster. Verarbeitet werden können außerdem Eindrücke, die die handelnden Polizeibeamten bei einer vorausgegangenen Identitätskontrolle gewinnen (BayVerfGH a. a. O.).

c) Einführung von § 202 Absatz 2 Nummer 4 LVwG-Entwurf

§ 202 Absatz 2 Nummer 4 LVwG-Entwurf übernimmt den Regelungsgehalt des bisherigen § 202 Absatz 2 Nummer 3 LVwG und wird redaktionell an die Weiterentwicklung der europäischen Rechtsgrundlagen für das Schengener Informationssystem angepasst.

14. Zu Nummer 14 (Änderung der Nummernfolge der Änderungsbefehle)

Der Änderungsantrag bedingt eine Änderung der Nummernfolge der Änderungsbefehle der Drs. 20/4284. Die bisherigen Nummer 16, 17 und 18 werden zu Nummern 29, 30 und 31.

15. Zu Nummer 15 (Änderung von § 206 LVwG und § 206a LVwG sowie Einführung eines § 213a LVwG-Entwurf)

a) Änderung des § 206 LVwG

§ 206 LVwG regelt Befugnisse der Polizei zur Durchsuchung von Sachen. Innerhalb der sachbezogenen Durchsuchungsbefugnisse sind zwei Kategorien zu unterscheiden. § 206 Nummer 1 LVwG gestattet die Durchsuchung von Sachen im Zusammenhang mit der Durchsuchung von Personen, und zwar in Bezug auf solche Sachen, die eine zu durchsuchende Person mitführt. Diese Durchsuchungsbefugnis ist akzessorisch in dem Sinne, dass sich die Voraussetzungen für die Durchsuchung der Sache nach denen der Durchsuchung der Person (§ 202 LVwG) richten, welche die Sache mit sich führt. Die weiteren sachbezogenen Durchsuchungsbefugnisse des § 206 Nummer 2 bis 6 LVwG sind dagegen unabhängig von der Durchsuchung der Person, welcher die Sache zuzuordnen ist. Diese selbständigen Befugnisse beziehen sich – ähnlich wie die zur Durchsuchung von Personen – teils auf die Vorschrift über

Identitätsfeststellungen in § 181 LVwG. So wird in § 206 Nummern 4 und 5 LVwG die Durchsuchung von Sachen gestattet, die an gefährlichen oder gefährdeten Orten (§ 181 Absatz 1 Satz 2 Nummern 2 und 3 LVwG) zurückgelassen vorgefunden werden. § 206 Nummer 6 LVwG regelt die Durchsuchung von Fahrzeugen an Kontrollstellen, in denen sich Personen befinden, deren Identität nach § 181 Absatz 1 Satz 2 Nummer 4 LVwG festgestellt werden kann. Hieran schließt die Erweiterung der Vorschrift an. Auch für die Kontrollsituation gemäß § 181 Absatz 1 Satz 2 Nummer 5 LVwG wird eine sachbezogene Durchsuchungsbefugnisse ergänzt.

§ 206 **Nummer 7** LVwG-Entwurf ermöglicht zukünftig die Durchsuchung von Fahrzeugen, in denen sich Personen befinden, deren Identität gemäß § 181 Absatz 1 Satz 2 Nummer 5 LVwG (bei Kontrollen in öffentlichen Einrichtungen des internationalen Verkehrs sowie auf Durchgangsstraßen zum Zwecke der Bekämpfung der grenzüberschreitenden Kriminalität oder von Straftaten von erheblicher Bedeutung) festgestellt werden darf. Es kommt dabei nicht darauf an, ob in den einschlägigen Fällen das Fahrzeug – durch die Person, deren Identität festgestellt wird – im Sinne von § 206 Nummer 1 LVwG „mitgeführt“ wird. Nach Maßgabe der obergerichtlichen Rechtsprechung ist der Durchsuchung von Fahrzeugen in diesen Konstellationen – nicht anders als der Durchsuchung der Person und im Unterschied zur bloßen Identitätsfeststellung – ein erhöhtes Eingriffsgewicht zuzumessen (BayVerfGH, Entscheidung v. 7. Feb. 2006, Vf. 69-VI-04 = NVwZ 2006, 1284 [1286]). Daher müssen für eine Durchsuchung des Fahrzeuges die Voraussetzungen für die Durchsuchung der Person nach § 202 Absatz 2 Nummer 3 LVwG-Entwurf vorliegen.

b) Änderung des § 206a LVwG

Die Änderung dient – wie die Änderung in Bezug auf § 202 Absatz 2 Nummer 4 LVwG – der redaktionellen Anpassung an die Weiterentwicklung der europäischen Rechtsgrundlagen für das Schengener Informationssystem.

c) Einführung eines § 213a LVwG-Entwurf

Mit § 213a LVwG-Entwurf wird eine Standardermächtigung zur Abwehr unbemannter Fahrzeugsysteme eingeführt.

Die Landespolizei ist bereits jetzt rechtlich in der Lage, unbemannte Fahrzeugsysteme – insbesondere Fluggeräte, sogenannte Drohnen – effektiv abzuwehren. Sie kann sich dazu auf die gefahrenabwehrrechtliche Generalklausel stützen. Die **Schaffung einer Standardbefugnis** bietet jedoch verschiedene Vorteile: Die Handlungsmöglichkeiten der Polizei zum Einsatz von Einsatzmitteln gegen unbemannte Fahrzeugsysteme, insbesondere Drohnen, erhalten eine klare und spezifische rechtliche Grundlage. Zudem verdeutlicht die Standard-

befugnis, dass zur Abwehr unbemannter Fahrzeugsysteme regelmäßig unmittelbar gegen die Sache selbst vorgegangen werden muss, weil der Fahrzeugsteuerer (zum Beispiel ein Drohnenpilot) oder andere als Störer heranzuziehende Personen nicht rechtzeitig festgestellt werden können. Dies steht zwar der Abwehrhandlung, die im Wege des Sofortvollzugs gemäß § 230 LVwG ausgeführt werden kann, prinzipiell nicht entgegen. Wenn es jedoch der spezifischen Gefahrenlage entspricht, dass Polizeiverfügungen typischerweise nicht erlassen werden können, ist es letztlich überzeugender eine Standardbefugnis in Gestalt einer sogenannten Ausführungsermächtigung vorzusehen. Das heißt, die Vorschrift verleiht auch die Befugnis, die Abwehrmaßnahme unmittelbar durch Realakt auszuführen, ohne dass es einer vorausgehenden Verfügung bedarf (vgl. dazu Schenke, Polizei- und Ordnungsrecht, 12. Aufl. 2023, Rn. 115).

aa) Gesetzgebungskompetenz

Das Land kann die Standardbefugnis, die dem allgemeinen Gefahrenabwehrrecht zuzurechnen ist, auf Grundlage von Artikel 70 Absatz 1 GG normieren (vgl. in Bezug auf die Abwehr unbemannter Fluggeräte: Becker/Gräber, NVwZ 2025, 1860; a. A. Thiel/Probst, KriPoZ 2025, 403). Der Umstand, dass die Befugnis zur Abwehr von Gefahren ermächtigt, die von (unbemannten) Fahrzeugen ausgehen, führt nicht dazu, dass die Regelungsmaterie insgesamt dem Luftverkehr (Artikel 73 Absatz 1 Nummer 6 GG) beziehungsweise dem Wasser- oder Straßenverkehr (Artikel 74 Absatz 1 Nummer 21 und 22 GG) zuzuordnen ist. Diese Kompetenztitel des Bundes erstrecken sich nur auf verkehrsspezifische Gefahren.

Der Kompetenztitel **Luftverkehr** (Artikel 73 Absatz 1 Nummer 6 GG) umfasst als Annex auch Regelungen zur Abwehr von Gefahren, die aus dem Luftverkehr herrühren (vgl. etwa BVerfG, Beschl. v. 3. Jul. 2012, 2 PBvU 1/11 = BVerfGE 132, 1 [6 f.] Rn. 17 bis 19 m. w. N.). Der Umfang einer Annexkompetenz reicht jedoch stets nur so weit, wie der sie konstituierende grundgesetzliche Begründungszusammenhang gegeben ist. Denn stillschweigend mitgeschriebene Gesetzgebungsbefugnisse des Bundes dürfen nicht Rechtsetzungsbefugnisse, die das Grundgesetz ausdrücklich den Ländern zuweist, aushöhlen oder minimieren. Deshalb werden stillschweigend mitgeschriebene Bundeszuständigkeiten dort, wo die Verfassung ihre Annahme gestattet, in ihrem Umfang durch den sie legitimierenden Regelungszusammenhang des Grundgesetzes beschränkt (Uhle in: Dürig/Herzog/Scholz, 107. EL März 2025, GG, Art. 70 Rn. 64). Eine Annexkompetenz erfasst und legitimiert daher nur Regelungen, die in dem für sie konstitutiven funktionalen Zusammenhang zur ausdrücklich geschriebenen Bundeskompetenz stehen. Deshalb reichen Kompetenzen kraft Annex in aller Regel nur punktuell in den dem Bund nicht explizit zugewiesenen Kompetenzbereich hinein (Uhle in: Dürig/Herzog/Scholz a. a. O. Rn. 72; Rozek in: Huber/Voß-

kuhle, 8. Aufl. 2024, GG, Art. 70 Rn. 48; Degenhart in: Sachs, 10. Aufl. 2024, GG, Art. 70 Rn. 37; jeweils mit zahlreichen w. N.). Zu dem von Artikel 73 Absatz 1 Nummer 6 GG umfassten Kompetenzbereich zählen mithin zwar sowohl die Abwehr von Gefahren, die aus dem Luftverkehr resultieren als auch die Abwehr von Gefahren, die auf den Luftverkehr einzuwirken drohen. Jedoch gilt dies nur insoweit, als es sich tatsächlich um die Abwehr luftverkehrsspezifischer Gefahren handelt und nicht die allgemeine Gefahrenabwehr im Vordergrund steht (Heintzen in: Huber/Voßkuhle, 8. Aufl. 2024, GG, Art. 73 Rn. 57; und allgemein Rozek in: Huber/Voßkuhle a. a. O. Art. 70 Rn. 48; Uhle in: Dürig/Herzog/Scholz a. a. O. 73 Rn. 137).

Der Umfang der von dem in Artikel 74 Absatz 1 Nummer 21 GG verankerten Kompetenztitel des **Rechts des Wasserverkehrs** erfassten Gefahrenabwehr ist auf die Begründung zu § 181b LVwG-Entwurf zu verweisen.

Das in Artikel 74 Absatz 1 Nummer 22 Alternative 1 GG aufgeführte **Straßenverkehrsrecht** ist ein besonderes Ordnungsrecht (BVerfG, Beschl. v. 10. Dez. 1975, 1 BvR 118/71 = BVerfGE 40, 371 [380]). Seine Zielrichtung ist einerseits die Abwehr von Gefahren des Verkehrs, die anderen Verkehrsteilnehmerinnen und Verkehrsteilnehmern oder Dritten drohen, sowie von Gefahren für den Verkehr von außen. Andererseits soll die Sicherheit und Leichtigkeit des Straßenverkehrs gewährleistet werden. Nicht erfasst sind jedoch Normen des Gefahrenabwehrrechts, die sich zwar auf den Straßenverkehr auswirken, aber keine verkehrsspezifische Gefahr zu bekämpfen trachten (Wittreck in: Dreier, 3. Aufl. 2015, GG, Art. 74 Rn. 108; Kment in: Jarass/Pieroth/Kment, 18. Aufl. 2024, GG, Art. 74 Rn. 61).

Die Gefahren, um die es bei der Abwehr unbemannter Fahrzeugsysteme, insbesondere von Fluggeräten geht, bestehen zunächst in der Abwehr von Vorbereitungshandlungen für Sabotage; teils sind sie der hybriden Bedrohung zuzurechnen, deren Zielrichtung in der Verunsicherung und Einschüchterung besteht. Dass diese Phänomene, zum Beispiel vermittelt durch den Einsatz beziehungsweise Missbrauch unbemannter Fluggeräte erfolgen, genügt allein nicht dazu, sie dem Luftverkehr zuzurechnen. Ebenso würde zum Beispiel auch der Umstand, dass das Auskundschaften eines Schutzobjekts aus einem (fahrenden) Kraftfahrzeug oder aus dem öffentlichen Verkehrsraum heraus getätigt wird, nicht dazu genügen, diese Sachverhalte als straßenverkehrsspezifische Gefahrenlage einzustufen. Der rein instrumentelle Bezug einer Gefahr zu einem Fahrzeug, das der Annäherung an ein Schutzobjekt oder der Tarnung dient, begründet keine verkehrsspezifische Gefahr (vgl. in Bezug auf Wasserfahrzeuge siehe: Begründung zu § 181b LVwG-Entwurf).

Differenziert zu betrachten sind dagegen die mit Blick auf unbemannte Fahrzeugsysteme ebenfalls relevanten Sachverhalte, in denen das

Fahrzeug selbst zielgerichtet zur Verletzung von Rechtsgütern eingesetzt wird. In dieser Konstellation kann in Bezug auf den Straßen- und Wasserverkehr eine verkehrsspezifische Gefahr vorliegen. Denn diese Regelungsmaterien erfassen in einem weiten Umfang auch Gefahren, die vom Straßen- oder Wasserverkehr für Dritte (außerhalb des Straßen- oder Wasserverkehrs) ausgehen (vgl. zum Straßenverkehrsrecht: Uhle in: Dürig/Herzog/Scholz, 108. EL August 2025, GG, Art. 74 Rn. 526 mit zahlreichen w. N.; zum Recht des Wasserverkehrs: BVerwG, Urt. v. 28. Okt. 1999, 7 A 1/98 = NVwZ 2000, 433 [434]). § 213a Absatz 1 Satz 3 LVwG-Entwurf stellt den Anwendungsvorrang des speziellen Gefahrenabwehrrechts insofern klar.

Anders zu beurteilen ist der Einsatz von unbemannten Fluggeräten. Nach Maßgabe der Rechtsprechung des BVerfG ist hinsichtlich der Abwehr der von Luftfahrzeugen ausgehenden (nicht betriebsbedingten) Gefahren eine aus Artikel 73 Absatz 1 Nummer 6 GG abgeleitete Annexkompetenz dann angezeigt, wenn eine dezentrale Regelungskompetenz mit dem Risiko einer unzureichend abwehrwirksamen Regelung verbunden ist, weil die Verwirklichung der Gefahr nicht auf ein Bundesland beschränkt bliebe (BVerfG, Beschl. v. 3. Jul. 2012, 2 PBvU 1/11 = BVerfGE 132, 1 [6 f.] Rn. 17 bis 19). Der Begründungszusammenhang bezieht sich dabei explizit auf katastrophenhafte Sachlagen im Sinne der Artikel 35 Absatz 2 Satz 2 und Absatz 3 GG. Das BVerfG stellt dabei insbesondere heraus, dass es gerade wegen der ausschließlichen Gesetzgebungskompetenz des Bundes eine strenge Prüfung des Zusammenhanges zwischen der Zuständigkeit des Bundes für ein bestimmtes Sachgebiet und der einschlägigen gefahrenabwehrrechtlichen Regelungen bedarf. Der Kreis verkehrsspezifischer Gefahren ist in Bezug auf den Luftverkehr daher prinzipiell enger. Dem entspricht, dass neben den betriebsbedingten Gefahren die Luftsicherheitsbehörden für die Gefahrenabwehr nach Maßgabe des Luftsicherheitsgesetzes (LuftSiG) im Kern nur für das Flugplatzgelände zuständig sind (vgl. § 16 Absatz 1 Satz 1 LuftSiG); außerhalb von Flugplätzen regelt das LuftSiG nur noch den Fall eines erheblichen Luftzwischenfalls, der einen besonders schweren Unglücksfall im Sinne von Artikel 35 Absatz 2 Satz 2 oder Absatz 3 GG vertypt (§§ 13 bis 15a LuftSiG).

bb) Zu § 213a Absatz 1 LVwG-Entwurf

§ 213a Absatz 1 **Satz 1** LVwG-Entwurf setzt für ein polizeiliches Einschreiten voraus, dass von einem unbemannten Fahrzeugsystem eine konkrete Gefahr für die öffentliche Sicherheit ausgeht. Einschreitschwelle ist mithin eine Sachlage, die bei ungehindertem Geschehensablauf in absehbarer Zeit mit hinreichender Wahrscheinlichkeit zu einem Schaden für das Schutzgut der öffentlichen Sicherheit führt. In welcher Ausprägung die öffentliche Sicherheit durch unbemannte Fahrzeugsysteme verletzt werden kann, hängt vom Einzelfall ab. In Betracht

kommen physische Verletzungen von Personen oder Sachwerten durch den gezielten Missbrauch oder als Folge einer leichtfertigen oder unbedachten Nutzung dieser Geräte. Die öffentliche Sicherheit kann jedoch auch in der Form verletzt sein, dass ex ante die Wahrscheinlichkeit der Verwirklichung von Straftatbeständen besteht. Dies kommt etwa bei Überflügen bestimmter Gebiete oder Objekte – wie Sabotageobjekten (also Gegenständen, auf die sich eine Sabotagehandlung gemäß § 87 Absatz 2 StGB möglicherweise beziehen kann) oder militärischen Einrichtungen oder Anlagen oder bestimmten Gebieten, die Bedeutung für die Sicherheit der Bundesrepublik Deutschland haben – in Betracht, bei denen nach Lage der Dinge ein Auskundschaften im Sinne von § 87 Absatz 1 Nummer 2 StGB oder ein sicherheitsgefährdendes Abbilden gemäß § 109g StGB möglich erscheint.

Auf Grundlage von § 213a Absatz 1 Satz 1 LVwG-Entwurf darf die Polizei die Fernsteuerung des Fahrzeugsystems unterbrechen oder die Steuerung übernehmen. Ferner darf sie auf das unbemannte Fahrzeugsystem mechanisch einwirken und es dabei beschädigen oder zerstören. Als Einsatzmittel darf die Polizei technische Mittel und Mittel des unmittelbaren Zwangs verwenden. Bei den technischen Mitteln handelt es sich insbesondere um Mittel, durch die in den Betrieb der Drohne eingegriffen werden kann, ohne diese physisch zu zerstören sowie um technische Maßnahmen zur Beeinflussung der Steuerungssysteme. Beispielhaft ist hier der Einsatz von Störsendern (sogenannter Jammer). Von diesen technischen Mitteln sind die Mittel des unmittelbaren Zwangs abzugrenzen, die in § 251 LVwG definiert sind. Zu ihnen zählen insbesondere klassische ballistische Abwehrmittel einschließlich Schusswaffen. Auch Netzwerfer oder Lasersysteme sind unter die Mittel des unmittelbaren Zwangs zu fassen (vgl. Schramm in DVBl. 2026, S. 146 [149].)

Gemäß § 213a Absatz 1 **Satz 2** LVwG-Entwurf wird klargestellt, dass die Polizei zur Abwehr unbemannter Fahrzeugsysteme ihrerseits solche Fahrzeugsysteme einsetzen darf.

§ 213a Absatz 1 **Satz 3** LVwG-Entwurf grenzt die allgemein-polizeiliche Befugnis als Teil des allgemeinen Gefahrenabwehrrechts gegenüber den spezielleren gefahrenabwehrrechtlichen Befugnissen des Rechts des Straßenverkehrs, des Luftverkehrs und der Schifffahrt ab, die als spezielles Gefahrenabwehrrecht Anwendungsvorrang haben. Dies gilt insbesondere soweit die Sicherheit und Ordnung des Straßen- respektive Wasserverkehrs im Einzelfalle konkrete betroffen ist (in Bezug auf § 44 Absatz 2 der Straßenverkehrsordnung beziehungsweise § 3 Absatz 1 Satz 1 SeeAufgG). Hinsichtlich unbemannter Fluggeräte gilt dies auf Grundlage von § 3 Absatz 1 LuftSiG soweit Flugplatzgelände betroffen sind (§ 16 Absatz 1 Satz 1 LuftSiG).

cc) Zu § 213a Absatz 2 und 3 LVwG-Entwurf

§ 213a **Absatz 2** LVwG hebt klarstellend hervor, dass bei Abwehrmaßnahmen gegen unbemannte Fahrzeugsysteme die Folgen, die das Einschreiten der Polizei in concreto für Rechtsgüter Dritter haben können (etwa beim Abschuss einer Drohne eine mögliche Gefährdung von Personen durch herabfallende Teile) in die Prüfung der Verhältnismäßigkeit im engeren Sinne beziehungsweise der Angemessenheit einzubeziehen sind. Dieser Aspekt prägt sowohl das Entschließungs- als auch das Auswahlermessen.

§ 213a **Absatz 3 Satz 1** LVwG-Entwurf gestattet den Einsatz technischer Mittel, um unbemannte Fahrzeugsysteme, von denen eine Gefahr für die öffentliche Sicherheit ausgehen kann, zu erkennen. Diese Detektion von unbemannten Fahrzeugsystemen findet im Vorfeld einer Gefahrenlage statt, erfordert weder eine konkrete Gefahr noch einen Gefahrenverdacht. § 213a Absatz 3 Satz 1 LVwG-Entwurf ermöglicht auf diese Weise ein unbemanntes Fahrzeug oder Gerät in einer frühen Phase festzustellen und daran anschließend eine Gefährdungsbeurteilung zu erstellen, die Grundlage für eine Abwehrmaßnahme gemäß § 213a Absatz 1 LVwG-Entwurf sein kann.

Die Vorverlagerung ist dadurch gerechtfertigt, dass die Detektion von unbemannten Fahrzeugsystemen durch Mittel erfolgen kann, die nicht auf personenbezogene Daten zugreifen und auch sonst typischerweise nicht in Grundrechte eingreifen. Beispielhaft sind hier neben der optischen Wahrnehmung durch den Menschen optische Systeme (zum Beispiel Kamera, Infrarottechnik), Radar sowie technische Mittel zur Signalaufklärung zu nennen. Eine Verarbeitung personenbezogener Daten ist auf Grundlage von § 213a Absatz 3 LVwG nicht zulässig, sondern müsste – wie § 213a **Absatz 3 Satz 2** LVwG-Entwurf klarstellt – auf eine andere Rechtsgrundlage gestützt werden, wie zum Beispiel § 185d LVwG-Entwurf oder § 185a LVwG, sofern auf Telekommunikationsdaten zugegriffen wird.

16. Zu Nummer 16 (Anpassung der Normierung der Drs. 20/4284)

Der Änderungsantrag bedingt eine Änderung der Nummernfolge der Änderungsbefehle der Drs. 20/4284. Die bisherige Nummer 19 wird zu Nummer 35.

Birte Glißmann **Jan Kürschner**

und Fraktion **und Fraktion**