

Landesbeauftragte für Datenschutz · Postfach 71 16 · 24171 Kiel

Innen- und Rechtsausschuss
des Schleswig-Holsteinischen Landtages
Herrn Vorsitzenden Jan Kürschner
Düsternbrooker Weg 70
24105 Kiel

nur per E-Mail: innenausschuss@landtag.ltsh.de

Landesbeauftragte für Datenschutz
Holstenstraße 98
24103 Kiel
Tel.: 0431 988-1200
Fax: 0431 988-1223
Ansprechpartner/in:
Barbara Körffer
Durchwahl: 988-1216
Aktenzeichen:
LD5-74.13/25.006

Kiel, 11. September 2026

Gesetz zur Fortentwicklung polizeirechtlicher Maßnahmen für einen wirksamen Schutz der öffentlichen Sicherheit

Gesetzentwurf der Landesregierung – Drucksache 4284; Änderungsantrag der Fraktionen von CDU und BÜNDNIS 90/DIE GRÜNEN – Umdruck 20/6786

Sehr geehrter Herr Vorsitzender,
sehr geehrte Damen und Herren Abgeordnete,

ich bedanke mich für die Gelegenheit, zu dem oben genannten Gesetzentwurf Stellung zu nehmen.

Mit dem Gesetzentwurf ist die Erweiterung bestehender Eingriffsbefugnisse und die Einführung neuer Befugnisse geplant, die für sich genommen und in ihrer Gesamtheit zu weitreichenden Grundrechtseingriffen mit großer Streubreite führen können.

Insbesondere Maßnahmen wie Gesichtserkennung durch biometrische Fernidentifizierung in Echtzeit oder nachträglich durch Auswertung von Daten aus dem Internet, Verhaltenserkennung bei Videoüberwachung im öffentlichen Raum oder im Straßenverkehr zur Erkennung von Ablenkungsverstößen, aber auch die automatisierte Datenanalyse können jede und jeden treffen, völlig unabhängig davon, ob die Person einen Anlass für die Maßnahme gegeben hat. Gleichzeitig werden hierfür neue technische Verfahren, mit oder ohne KI, eingeführt, deren Treffergenauigkeit zum gegenwärtigen Zeitpunkt sicherlich nur schwer eingeschätzt werden kann. Fehl-Erkennungen können für die betroffenen Personen mit Folgen verbunden sein. Diese mögen bei dem Verdacht von Ablenkungsverstößen im Straßenverkehr noch überschaubar sein. Bei anderen Maßnahmen, etwa dem Einsatz einer Echtzeit-Fernidentifizierung zur Suche nach terroristischen Gefährdern, können Fehler in der Gesichtserkennung für falsch als gesuchte Gefährder identifizierte Personen gravierende Folgen haben.

Ich kann daher dem Gesetzgeber nur dazu raten, den Gesetzentwurf mit größter Sorgfalt zu prüfen. Die hohe Anzahl der von Ihnen eingeladenen Sachverständigen, die zu dem Vorha-

ben angehört werden, ist für mich ein Zeichen, dass Sie die Auswirkungen auf die Grundrechte der Bürgerinnen und Bürger ernst nehmen und den Entwurf mit der gebotenen Sorgfalt prüfen.

Zu der Prüfung gehören ebenso die Frage der Erforderlichkeit und Eignung der vorgeschlagenen Maßnahmen zur Erreichung des vorgesehenen Ziels wie die Verhältnismäßigkeit der Befugnisnormen, d.h. die Prüfung der Eingriffsvoraussetzungen und die Regelung flankierender grundrechtsschützender Maßnahmen. Die Folgen der neuen Technologien, die für die neuen Befugnisse angeschafft und eingesetzt werden, lassen sich heute noch nicht vollständig in allen Einzelheiten abschätzen. Aufgrund dieser Unsicherheit in Bezug auf die Technologien, aber auch in Bezug auf die Einsatzpraxis bei den Polizeibehörden, sollte der Landtag die Wirksamkeit und die Auswirkung der neuen Befugnisse auf die Grundrechte nach einer ersten Phase der praktischen Anwendung erneut überprüfen. Ich rate daher dringend, die Befugnisse zeitlich zu befristen und unter den Vorbehalt einer positiven Evaluierung zu stellen.

Zur Erforderlichkeit und Eignung der vorgeschlagenen Änderungen

Anlass für die Änderungen ist nach der Entwurfsbegründung der Anstieg der Messerangriffe in Schleswig-Holstein. Damit dient der Gesetzentwurf einer gewichtigen staatlichen Aufgabe, und es ist zweifellos Aufgabe des Gesetzgebers, auf neue oder ansteigende Kriminalität zu reagieren. Jedoch wird aus der Entwurfsbegründung nicht deutlich, wie die geplanten Maßnahmen zur Eindämmung von Messerangriffen oder anderen ähnlich schwerwiegender Kriminalitätsphänomenen beitragen können. Während die Entwurfsbegründung erkennen lässt, dass die rechtlichen Anforderungen für die Maßnahmen, z. B. aus der Rechtsprechung des Bundesverfassungsgerichts und aus der KI-Verordnung der EU, eingehend geprüft und berücksichtigt worden sind, bleibt die Darlegung der fachlichen Eignung und Erforderlichkeit der geplanten Maßnahmen abstrakt. Die verfassungsrechtliche Verhältnismäßigkeit der geplanten Maßnahmen, d. h. Geeignetheit, Erforderlichkeit und angesichts der hohen Eingriffsintensität auch die Angemessenheit, ist daher schwer nachvollziehbar. Dabei fällt auf, dass es zwar einzelne Maßnahmen gibt, für die der fachliche Nutzen konkreter und damit auch nachvollziehbarer dargelegt ist. Dies gilt z. B. für den Einsatz der Mustererkennung bei der Videoüberwachung. Insbesondere aber für die besonders schwerwiegenden Eingriffsbefugnisse, wie die biometrische Echtzeit-Fernidentifizierung oder die automatisierte Datenanalyse, wird der fachliche Bedarf hingegen nicht konkret dargelegt.

Zu den einzelnen Regelungen

Bei der Durchsicht des Entwurfs sind einige Punkte aufgefallen, in denen aus meiner Sicht Nachbesserungsbedarf besteht.

Zum Gesetzentwurf der Landesregierung – Drs. 20/4284

Zur Videoüberwachung, § 184 LVwG-E

Durch die im Gesetzentwurf vorgesehenen Neuerungen werden Grundrechtseingriffe für Bürgerinnen und Bürger im Zusammenhang mit Videoüberwachung in einem erheblichen Maße erweitert. So sollen während der Videoüberwachung Verfahren der Mustererkennung und der biometrischen Fernidentifizierung eingesetzt werden dürfen. Zudem sollen die Videoaufzeichnungen für nachträgliche biometrische Abgleiche im Wege der Fernidentifizierung nutzbar gemacht werden.

Gleichzeitig sind in § 184 Abs. LVwG-E erhebliche Ausweitungen des Einsatzes von Videoüberwachungsmaßnahmen im öffentlichen Raum vorgesehen. Nach dem geltenden Recht ist

dieser Einsatz nur in engen Grenzen bei Veranstaltungen oder an Kriminalitäts- und Gefahrenschwerpunkten zulässig. Im Gesetzentwurf werden die Voraussetzungen für den Einsatz deutlich herabgesenkt. Dies führt in Kombination mit dem höheren Eingriffsgewicht der Videoüberwachung zu einer deutlichen Ausweitung und Vertiefung von Grundrechtseingriffen.

Die Verhältnismäßigkeit dieser Ausweitung ist insbesondere in folgenden Punkten zweifelhaft:

Nach **§ 184 Abs. 3 Satz 1 Nr. 1 LVwG-E** soll eine Videoaufzeichnung an allgemein zugänglichen Plätzen erlaubt werden, wenn dies zur Abwehr einer Gefahr für die öffentliche Sicherheit zulässig ist. Damit würde der Anwendungsbereich der Videoüberwachung mit Aufzeichnung im öffentlichen Raum durch Polizei- und Ordnungsbehörden erheblich erweitert. Es reicht danach eine Gefahr für jedes beliebige Rechtsgut der öffentlichen Sicherheit aus. Angesichts der großen Anzahl betroffener Personen bei der Videoüberwachung im öffentlichen Raum ist es fraglich, ob die Eingriffsvoraussetzungen verhältnismäßig sind. Zur Wahrung der Verhältnismäßigkeit sollte die Befugnis auf Gefahren für besonders gewichtige Rechtsgüter beschränkt werden.

§ 184 Abs. 3 Satz 1 Nr. 2 LVwG-E erlaubt Videoüberwachung, wenn Tatsachen die Annahme rechtfertigen, dass an dem Ort Ordnungswidrigkeiten von erheblicher Bedeutung oder Straftaten begangen werden. Auch hierdurch wird der Anwendungsbereich der Videoüberwachung erheblich ausgeweitet. Es reicht dafür eine jegliche Straftat unabhängig von ihrem Schweregrad aus: Auch an die Häufung von Straftaten oder Ordnungswidrigkeiten werden keine Anforderungen gestellt, mit der Ausnahme, dass es wohl mehrere Straftaten oder Ordnungswidrigkeiten sein müssen. Hier sollten zur Wahrung der Verhältnismäßigkeit weitere Voraussetzungen im Hinblick auf die Schwere und auf die Häufigkeit von Straftaten oder Ordnungswidrigkeiten vorgesehen werden.

§ 184 Abs. 6 Nr. 2 LVwG-E erlaubt eine längere Speicherung der Videoaufzeichnungen, wenn Tatsachen dafür sprechen, dass die Person künftig vergleichbare Straftaten oder Straftaten im Sinne des § 179 Absatz 2 LVwG begehen wird. Die Regelung entspricht dem geltenden Recht, doch durch die neu vorgesehenen Möglichkeiten der biometrischen Fernidentifizierung erhöht sich für diese Aufzeichnungen ebenfalls das Eingriffsgewicht. Daher bedarf auch die geltende Regelung einer neuerlichen Überprüfung. Dabei ist zunächst die Erforderlichkeit der Speicherung unklar. Es ist nicht ohne Weiteres nachvollziehbar, wie eine Speicherung der Aufzeichnungen zur Abwehr künftiger Gefahren beitragen kann. Des Weiteren ist eine zeitliche Begrenzung dieser Speicherung nicht geregelt. Während sich bei den anderen Alternativen des Absatzes 6 Satz 2 LVwG-E die Löschpflicht aus dem Speicheranlass ergibt (da im Falle der Nummer 1 die Aufbewahrung bzw. Löschung an das Straf- oder Ordnungswidrigkeitenverfahren gekoppelt und im Falle der Nummer 2 die Daten für die Dauer der Überprüfung der Rechtmäßigkeit der polizeilichen Maßnahme bzw. so lange aufbewahrt werden, bis mit einer Überprüfung nicht mehr zu rechnen ist), fehlt ein Anknüpfungspunkt hierfür in dem Speicheranlass nach Absatz 6 Satz 2 Nr. 2. Es handelt sich hier um eine Speicherung zur Vorsorge. Daher wären für die Löschung ähnliche Regelungen wie für die Löschung in Dateien nach § 196 LVwG empfehlenswert.

Zur Echtzeit-Fernidentifizierung

Zu § 184b Abs. 1 LVwG-E

In der Regelung der Voraussetzungen für die biometrische Fernidentifizierung unter Einsatz eines KI-Systems wird auf die Verwendungsziele des Art. 5 Abs. 1 Buchst. h der KI-Verordnung (KI-VO) Bezug genommen. Diese Vorschrift in der KI-Verordnung enthält jedoch nicht

nur Verwendungsziele, sondern zum Teil auch spezifische Eingriffsschwellen. So wird insbesondere in der in Bezug genommenen Vorschrift des Art. 5 Abs. 1 Buchst. h Gliederungspunkt ii 2. Alternative KI-VO eine bestimmte Gefahr vorausgesetzt, nämlich eine tatsächliche und bestehende oder tatsächliche und vorhersehbare Gefahr eines Terroranschlags. Es geht aus der Formulierung des § 184b Abs. 1 Satz 3 LVwG-E nicht ausreichend klar hervor, dass diese tatsächliche und bestehende oder tatsächliche und vorhersehbare Gefahr vorliegen muss. Zwar werden in Satz 4 auch die weiteren in der KI-Verordnung genannten Voraussetzungen für anwendbar erklärt. Diese allgemeine Verweisung erfordert eine eigenständige Prüfung und Ableitung von Voraussetzungen durch die Normanwendenden und ist daher im Hinblick auf die Bestimmtheit der Norm zweifelhaft. Vorzugswürdig wäre eine abschließende, für die Normanwendenden hinreichend klare, Regelung aller Eingriffsvoraussetzungen im LVwG.

Zur nachträglichen Fernidentifizierung

Zu § 195b LVwG-E

Für den hier geregelten Abgleich werden zunächst Daten aus dem Internet zusammengetragen und gespeichert. Damit ist das Verbot der Erstellung von Datenbanken zur Gesichtserkennung nach Art. 2 Abs. 1 Buchstabe e der KI-VO berührt. Dieses Verbot gilt nur für Datenbanken, die durch das ungezielte Auslesen von Gesichtsbildern aus dem Internet erstellt werden. Damit das Verbot nicht zum Tragen kommt, ist es also wichtig, dass die abzugleichenden Daten gezielt aus dem Internet erhoben werden. Nach der Mitteilung der Europäischen Kommission zum Verbot von Datenbanken zur Gesichtserkennung nach Art. 5 der KI-VO (Leitlinien der Kommission zu verbotenen Praktiken der künstlichen Intelligenz gemäß der Verordnung (EU) 2024/1689 (KI-Verordnung) vom 29.7.2025, C(2025) 5052 final) bezieht sich „ungezielt“ auf eine Technik, die wie ein Staubsauger funktioniert und so viele Daten und Informationen wie möglich aufnimmt, ohne auf speziell und individuell bestimmte Subjekte für das Auslesen abzielen. Demnach bedeutet der Begriff „ungezielt“, dass kein besonderer Schwerpunkt auf bestimmte Einzelpersonen oder eine bestimmte Gruppe von Einzelpersonen gelegt wird (KOM, a.a.O. Rn. 228). Wird hingegen ein Ausleseinstrument angewiesen, nur Bilder oder Videos zu sammeln, die menschliche Gesichter von bestimmten Personen oder einer vordefinierten Gruppe von Personen enthalten, dann erhält das Auslesen ein Ziel, beispielsweise einen bestimmten Straftäter zu finden oder eine Gruppe von Opfern zu identifizieren. Ein solches Auslesen fällt nicht unter das Verbot (KOM, a.a.O. Rn. 229).

Diese Einschränkungen sind in der Regelung in § 195 Abs. 1 LVwG-E für die Daten, die aus dem Internet erhoben werden dürfen, nicht ausreichend abgebildet. Es wird lediglich der Zweck des Abgleichs beschreiben. Anforderungen an die Auswahl der Daten fehlen hingegen. Nach den Erläuterungen der Kommission ist aber eine anlassbezogene Beschränkung bei der Zusammenstellung der Daten aus dem Internet erforderlich, um nicht dem Verbot des Art. 5 Abs. 1 Buchst. e KI-VO zu unterfallen. Dementsprechend müssten in § 195b LVwG-E Anforderungen an die spezifische Selektion der aus dem Internet zu erhebenden Daten ergänzt werden.

Zur automatisierten Datenanalyse

Zu § 188c Abs. 3 LVwG-E

Die hier geregelte Datenanalyse wird in der Begründung als Datenanalyse mit reduziertem Eingriffsgewicht beschrieben. Ausschlaggebend für das geringe Eingriffsgewicht soll nach der Begründung unter anderem die Beschränkung der Datenquellen sein. In die Datenanalyse

nach Absatz 3 sollen personenbezogene Daten aus Vorgangsbearbeitungs- und Fallbearbeitungssystemen, polizeilichen Auskunft-, Kommunikations-, Einsatzleit- und Einsatzdokumentationssystemen sowie Asservaten einbezogen werden können. Hinzu kommen nach Absatz 5 Datensätze aus gezielten Abfragen gesondert geführter staatlicher Register und einzelne gesondert gespeicherte Datensätze aus Internetquellen.

Der Ansatz, abgestufte Maßnahmen mit jeweils unterschiedlichen Eingriffsschwellen vorzusehen, ist grundsätzlich zu begrüßen. Er entspricht den Vorgaben des Bundesverfassungsgerichts aus der Entscheidung vom 16.2.2023 (Hessendata). Es ist jedoch zweifelhaft, ob mit der Beschränkung auf die in Absatz 3 genannten Datenquellen schon eine nennenswerte Reduzierung der Datenmenge und des Eingriffsgewichts erreicht wird, sodass die Maßnahmen durch die vorgesehenen niedrigeren Eingriffsvoraussetzungen gerechtfertigt werden kann. Denn die genannten Datenquellen dürften bereits nahezu die gesamten tatsächlich vorhandenen Daten umfassen. In die Datenanalyse mit hohem Eingriffsgewicht nach Absatz 4 können zusätzlich zu den in Absatz 3 genannten Daten solche aus Wohnraumüberwachungen und Online-Durchsuchungen sowie unbeschränkt Verkehrsdaten aus Funkzellenabfragen einbezogen werden. Damit unterscheidet sich die Datenanalyse nach Absatz 3 nicht wesentlich von der Datenanalyse nach Absatz 4, insbesondere da Maßnahmen der Wohnraumüberwachung und Online-Durchsuchung äußerst selten angewandt werden und der Datenbestand daher allenfalls gering sein dürfte.

Nach der Rechtsprechung des Bundesverfassungsgerichts liegt ein schwerer Eingriff in das Recht auf informationelle Selbstbestimmung vor, wenn unter anderem Personen vermehrt dem Risiko gegen sie gerichteter polizeilicher Ermittlungsmaßnahmen ausgesetzt werden, die objektiv nicht zurechenbar in das relevante Geschehen verfangen sind (BVerfG, Urteil vom 16.2.2023, 1 BvR 1547/19 und 1 BvR 2634/20, Rn. 73, 77). Dies ist hier insbesondere aufgrund der Einbeziehung der Datenbestände des Vorgangsbearbeitungssystems zu befürchten. Denn dadurch wird eine große Menge von Personen in die Analyse einbezogen, die nicht selbst Beschuldigte einer Straftat oder Verursachende einer Gefahr sind, sondern z. B. Anzeigende, Geschädigte, Zeuginnen und Zeugen oder Hinweisgebende. Auch werden Sachverhalte einbezogen, die für den Schutz der in Absatz 3 genannten Rechtsgüter keine Relevanz haben. Denn im Vorgangsbearbeitungssystem sind auch Bagatelldelikte und Ordnungswidrigkeiten sowie alle Einsatzberichte der Polizei gespeichert, beispielsweise wegen Ruhestörungen oder vermissten Personen ohne Anhaltspunkte für Straftaten. Dies dürfte eine große Anzahl von Personen betreffen. Zudem dürfen nach Absatz 5 auch Datenbestände aus anderen Quellen einbezogen werden. Es ist daher zweifelhaft, ob die vorgesehenen Schwellen für die Analyse dieser Daten verhältnismäßig sind.

Eine deutliche Abstufung könnte erreicht werden, indem die Datenquellen für die Analyse mit reduziertem Eingriffsgewicht weiter beschränkt würden. Dafür würde sich vor allem eine Differenzierung nach Personengruppen bzw. Rollen anbieten. Eine wesentliche Reduzierung des Eingriffsgewichts würde erreicht, wenn die Daten von nicht anlassgebenden Personen – wie Geschädigten, Zeuginnen und Zeugen, Anzeigenden oder Hinweisgebenden – aus dem Datenbestand für die Analyse mit reduziertem Eingriffsgewicht herausgenommen würden. Bei der Durchführung der Analyse ist ein gestuftes Vorgehen nach solchen Kategorien vorgesehen (siehe § 188d Abs. 2 LVwG-E). Dies sollte auch auf die Eingriffsvoraussetzungen in § 188c Abs. 3 LVwG-E übertragen werden.

Zum Änderungsantrag der Fraktionen von CDU und BÜNDNIS 90/DIE GRÜNEN – Um- druck 20/6786

Mit dem Änderungsantrag soll unter anderem die Befugnis zum Einsatz von Systemen zur Erkennung von Ablenkungsverstößen im Straßenverkehr eingeführt werden (§ 184d LVwG-E). Fahrzeugführende werden dazu gefilmt, und die Aufnahmen werden automatisiert im Hinblick darauf ausgewertet, ob mobile Geräte unbefugt genutzt werden. Gleichzeitig wird das Kfz-Kennzeichen erfasst.

Damit werden alle Fahrzeugführenden einer zu kontrollierenden Stichprobe in die Maßnahme einbezogen. Von ihnen werden Aufnahmen gefertigt und automatisiert sowie durch Beamte ausgewertet, und es wird das Kfz-Kennzeichen erhoben und kurzfristig gespeichert. Hierbei handelt es sich um einen Grundrechtseingriff von erheblicher Streubreite. Eine eigene Rechtsgrundlage ist hierfür erforderlich. Sie wird mit dem vorgelegten Entwurf vorgeschlagen. Der Zweck der Maßnahme kann nur in der Gefahrenabwehr liegen. Dies ergibt sich bereits aus der Gesetzgebungskompetenz des Landesgesetzgebers. Aber auch im Hinblick auf die Verhältnismäßigkeit wäre ein repressiver Zweck fragwürdig, denn Verstöße durch Nutzung von mobilen Geräten im Straßenverkehr sind regelmäßig Ordnungswidrigkeiten. Es wäre fraglich, ob Ordnungswidrigkeiten einen solch weitreichenden Eingriff in Grundrechte rechtfertigen könnten.

Der Schutz gewichtiger Rechtsgüter kommt hingegen grundsätzlich als Rechtfertigung des Grundrechtseingriffs in Betracht. Voraussetzung hierfür ist zunächst eine abstrakte Gefahrenlage durch unerlaubte Nutzung von Geräten am Steuer. Der Entwurfsbegründung sind hierzu keine substantziellen Angaben zu entnehmen; es wird auf eine vermutete hohe Dunkelziffer verwiesen. Des Weiteren muss die Maßnahme geeignet sein, Gefahren tatsächlich auch abzuwehren. Wie dies erfolgen soll, geht aus der Entwurfsbegründung nicht deutlich hervor. Da es sich bei der Gerätenutzung oftmals nur um kurzzeitige Nutzungen handeln wird, die oftmals auch bei einer umgehenden Kontrolle bereits beendet sein dürften, dürfte in der Praxis wohl häufig nur eine nachträgliche polizeiliche Maßnahme in Betracht kommen. Besteht diese Maßnahme in einer Geldbuße oder Verwarnung nach dem Ordnungswidrigkeitengesetz, verschwimmt die Abgrenzung zwischen präventivem und repressivem Einsatz.

Befristung und Evaluierung der Maßnahmen

In Anbetracht des erheblichen Eingriffsgewichts der neu einzuführenden Maßnahmen sollten diese zeitlich befristet und vor einer etwaigen Verlängerung evaluiert werden.

Für einen weiteren Austausch stehe ich mit meinem Team gern zur Verfügung.

Mit freundlichen Grüßen

gez. Dr. h. c. Marit Hansen
Landesbeauftragte für Datenschutz