



An den
Vorsitzenden des
Innen- und Rechtsausschuss des
Schleswig-Holsteinischen Landtages
Herrn Jan Kürschner, MdL

Telefon: 0431 880-5378
Telefax: 0431 880-5374
Durchwahl: 0431 880-1504
E-Mail: f.becker@law.uni-kiel.de
www.becker.jura.uni-kiel.de

per Mail: innenausschuss@landtag.ltsh.de

Schleswig-Holsteinischer Landtag Umdruck 20/7357

Gesetzentwurf der Landesregierung: Gesetz zur Fortentwicklung polizeirechtlicher Maßnahmen für einen wirksamen Schutz der öffentlichen Sicherheit (Drucksache 20/4284)

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

Sie haben mir freundlicherweise die Gelegenheit eingeräumt, zu dem o.a. Gesetzentwurf Stellung zu nehmen. Von dieser Gelegenheit mache ich gerne Gebrauch.

Ich darf eingangs allerdings darauf hinweisen, dass die Komplexität der vorgeschlagenen Änderungen nur eine punktuelle Befassung erlaubt, die auch nicht zu jedem einzelnen Aspekt die verfassungsrechtliche Problematik erschöpfend ausleuchten kann. Die nachfolgende Stellungnahme stellt daher keine eingehende unions- und verfassungsrechtliche Prüfung dar, sondern hebt nach summarischer Prüfung einzelne relevant erscheinende Aspekte exemplarisch hervor.

Ich habe bereits im Rahmen einer Verbändeanhörung zu dem Gesetzentwurf Stellung genommen. In dieser zweiten Stellungnahme möchte ich explizit diejenigen Fragen in den Vordergrund rücken, die mir zu dem Thema der biometrischen Fernidentifizierung gestellt wurden.

Meine Mitarbeiter Nico Arndt-Borgerding, Daniel Garschke, Felix Siegmon und Hannes Wittenberg haben mich bei der Erarbeitung dieser Stellungnahme maßgeblich unterstützt.

Inhaltsübersicht

I. Allgemeine verfassungsrechtliche und unionsrechtliche Rahmenbedingungen	4
1. Biometrische Fernidentifizierung in der Rechtsprechung des BVerfG	5
a) Vergleich mit der automatisierten Datenanalyse	5
b) Vergleich mit der Rasterfahndung	6
c) Kombination der verfassungsrechtlichen Anforderungen	7
d) Umsetzung in §§ 184b, 195b LVwG-E	8
2. Unionsrechtliche Rahmenbedingungen: KI-Verordnung	9
a) Biometrische Echtzeit-Fernidentifikation	10
aa) Unbedingte Erforderlichkeit zur Erreichung spezifischer Ziele	10
(1) Vorgaben	10
(2) Umsetzung	11
bb) Grundrechte-Folgenabschätzung und Registrierung des KI-Systems	13
b) Nachträgliche biometrische Fernidentifizierung	13
c) Verbot der Inbetriebnahme von Datenbanken zur Gesichtserkennung	13
II. Rechtsstaatliche Rahmenbedingungen	14
1. Überblick	14
2. Berichts- und Protokollierungspflichten	17
a) Berichtspflichten	17
b) Protokollierungspflichten	17
III. Unterscheidung der rechtlichen Anforderungen an eine Echtzeit- Fernidentifizierung und an eine nachträgliche Fernidentifizierung	18

IV. Verfassungsrechtliche Erheblichkeit der Herkunft von Referenzdaten für Fernidentifizierungen	21
V. Zeitliche Höchstdauer der Maßnahme und Befristung für Fernidentifizierungen	22
VI. Überprüfung der Ergebnisse	23
VII. § 184 LVwG-E	25
1. Ausweitung der Datenerhebung an allgemein zugänglichen Orten	25
2. Automatisierte Erkennung von Bewegungsmustern	25
VIII. Verfahren und technische Umsetzung	26
IX. Schlussbemerkung	27
X. Zusammenfassung der Ergebnisse	28

I. Allgemeine verfassungsrechtliche und unionsrechtliche Rahmenbedingungen

Die Erhebung personenbezogener Daten ist für die Effektivität der modernen Gefahrenabwehr unerlässlich. Gleichzeitig erweist sie sich aber aus rechtsstaatlicher Perspektive auch als besonders problematisch, weil in verschiedene und äußerst sensible Grundrechte eingegriffen werden kann (Allgemeines Persönlichkeitsrecht mit seinen verschiedenen Ausprägungen: Grundrecht auf informationelle Selbstbestimmung und Grundrecht der Integrität informationstechnischer Systeme; Brief- und Fernmeldegeheimnis; Unverletzlichkeit der Wohnung). Diese Grundrechte stellen wiederum je nach Situation ganz unterschiedliche Anforderungen an die Rechtfertigung eines Eingriffs. Bei der biometrischen Fernidentifizierung bildet vor allem das Grundrecht auf informationelle Selbstbestimmung den Maßstab (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG).

Die Nutzung von künstlicher Intelligenz (KI) zur Durchführung von biometrischen Echtzeit-Fernidentifizierungssystemen ist darüber hinaus durch die unionsrechtliche VO (EU) 2024/1689 (KI-VO) mit einem grundsätzlichen Verbot belegt, von dem nur in eng umgrenzten Ausnahmefällen abgewichen werden kann (Art. 5 Abs. 1 UAbs. 1 lit. h KI-VO). Wenn der schleswig-holsteinische Gesetzgeber von dieser Ausnahme Gebrauch macht, führt er i.S.v. Art. 51 Abs. 1 S. 1 GRCh Unionsrecht durch und ist dadurch an die europäischen Grundrechte gebunden. Der Gebrauch von dieser Ausnahme steht jedoch im mitgliedstaatlichen Ermessen, sodass primär die deutschen Grundrechte anwendbar sind, die den Standard der GRCh grundsätzlich mit gewährleisten (vgl. BVerfGE 152, 152 (LS. 1) – Recht auf Vergessen I). Nur wenn im Einzelfall Anhaltspunkte für einen höheren Schutzstandard durch die Unionsgrundrechte vorliegen, werden diese zum Prüfungsmaßstab (BVerfGE 152, 152 (180 ff.) Rn. 67 ff.).

Das Bundesverfassungsgericht (BVerfG) hat für die verschiedenen Konstellationen der Grundrechtseingriffe einen mittlerweile umfangreichen Katalog an Tatbestandsvoraussetzungen entwickelt, die jeweils eine spezifische Eingriffshürde abbilden. Gängig sind etwa die Begriffe der „hinreichend konkretisierten Gefahrenlage“, der „qualifizierte Tatverdacht“, der „Spurenansatz“ oder die „dringende Gefahr“ (Überblick mit Einzelnachweisen bei Wittenberg, NVwZ 2024, 1753 (1754 f.)).

Das Konvolut dieser verschiedenen Eingriffshürden macht es erforderlich, die konkret einzuhaltenden Standards bei der biometrischen Fernidentifizierung im Einzelnen zu ermitteln und auf ihre Einhaltung im Gesetzentwurf zu überprüfen.

1. Biometrische Fernidentifizierung in der Rechtsprechung des BVerfG

Das BVerfG hat sich bisher nicht ausdrücklich zu den Anforderungen an die biometrische Fernidentifizierung geäußert. Allerdings hat das Gericht in verschiedenen Entscheidungen Anforderungen an die Erhebung von personenbezogenen Daten, zu denen auch die biometrischen Daten gehören, präzisiert.

a) Vergleich mit der automatisierten Datenanalyse

Besonders wegweisend ist in dem Zusammenhang die Entscheidung des BVerfG zur automatisierten Datenanalyse in Hessen und Hamburg (BVerfGE 165, 363). Das Urteil betraf Regelungen, die die automatisierte Weiterverwendung und Zusammenführung von bereits erhobenen Daten ermöglichten.

Die vom BVerfG aufgestellten Maßstäbe können teilweise sinngemäß auf die biometrische Fernidentifizierung übertragen werden. Bei der Echtzeit-Fernidentifizierung werden neue biometrische Daten aus bestehenden Datensätzen extrahiert und daraufhin mit neuen Datensätzen, nämlich in Echtzeit erhobenen biometrischen Daten von Videoüberwachungen, abgeglichen. Bei der nachträglichen Fernidentifizierung erfolgt der Abgleich statt mit in Echtzeit erhobenen biometrischen Daten, mit biometrischen Daten, die aus Internetveröffentlichungen oder polizeilichen Datenbeständen extrahiert wurden. In beiden Fällen werden neue Daten erhoben und miteinander abgeglichen. Es handelt sich daher richtigerweise um ein mit der Datenanalyse in Teilen vergleichbares Verfahren (vgl. Teichmann, NJOZ 2026, 705 (708)).

Das BVerfG sieht in der automatisierten Datenanalyse gleich mehrere Grundrechtseingriffe in das Recht auf informationelle Selbstbestimmung. Einerseits werden nämlich Daten, die bereits erhoben worden sind, im Rahmen eines neuen Anlasses weiterverwendet (BVerfGE 165, 363 (Rn. 55 ff.)). Andererseits kommt der automatisierten Verknüpfung auch ein eigenständiges, über die Weiterverwendung hinausgehendes Eingriffsgewicht zu (BVerfGE 165, 363, Rn. 66 ff.). Die automatisierte Analyse ermöglicht es, große Datenbestände auszuwerten und damit persönlichkeitsrelevante Informationen zu erschließen, die mit herkömmlichen Methoden nicht zu erlangen wären (BVerfGE 165, 363 (396) Rn. 69). In diesen verbesserten Erkenntnismöglichkeiten liegt sodann auch der Grund für das eigenständige Eingriffsgewicht, welches nicht durch den Grundsatz der Zweckbindung abgegolten werden kann (BVerfGE 165, 363 (397 f.) Rn. 70). Darüber hinaus bestehen durch die weitergehende Automatisierung der Polizeiarbeit Diskriminierungsrisiken, die eine nach Art. 3 Abs. 1, 3 GG unzulässige Benachteiligung darstellen können (BVerfGE 165, 363 (400 f.) Rn. 77).

Die verfassungsrechtlichen Anforderungen an die Rechtfertigung hängen dann davon ab, wie eingriffsintensiv die konkreten Ermächtigungsgrundlagen ausgestaltet sind: Können etwa genaue Bewegungsprofile erstellt werden, handelt es sich um einen besonders intensiven Grundrechtseingriff (BVerfGE 165, 363 (Rn. 73)). In diesem Fall würden die Voraussetzungen für eingriffsintensive, heimliche Überwachungsmaßnahmen gelten: Es müsste ein “besonders gewichtiges Rechtsgut” geschützt werden und einer “hinreichend konkretisierten Gefahr” ausgesetzt sein (BVerfGE 165, 363 (Rn. 104 ff.); zum Grad der hinreichend konkretisierten Gefahr BVerfGE 141, 220 (272) Rn. 112).

Die biometrische Fernidentifizierung ermöglicht nicht das Erstellen von Verhaltens-, Beziehungs-, oder Bewegungsprofilen. Durch sie wird überprüft, wo die gesuchte biometrische Signatur aufzufinden ist. Es werden ansonsten keine neuen Informationen generiert. Insofern ist die Eingriffstiefe geringer im Vergleich zu dem, was bei der Datenanalyse generiert werden könnte. Dieses Minus wird jedoch durch andere Faktoren ausgeglichen. Die erhobenen und abgeglichenen Daten weisen biometrischen Charakter auf und haben durch ihre damit einhergehende Unveränderlichkeit ein hohes Eingriffsgewicht (vgl. Umkehrschluss aus BVerfGE 165, 363 (404) Rn. 87). Zusätzlich besteht eine sehr hohe Streubreite. Um die biometrische Signatur der gesuchten Person mit ihnen abgleichen zu können, müssen die biometrischen Daten von allen aufgezeichneten Personen erhoben werden. Dies geschieht ohne, dass die Betroffenen einen Anlass geboten haben und ohne deren Kenntnis.

Einen noch weiteren Betroffenenkreis betrifft die nachträgliche Fernidentifizierung. Für sie werden öffentlich zugängliche Daten aus dem Internet hinsichtlich ihrer biometrischen Aspekte ausgewertet. Somit sind bei der nachträglichen Fernidentifizierung potenziell alle Menschen betroffen, deren personenbezogenen Daten im Internet auffindbar sind. Dies kann bspw. auch Personen betreffen, die unwissentlich auf Fotos anderer Menschen zu sehen sind. Diese haben sich aber nicht aktiv dafür entschieden, öffentlich im Internet präsent zu sein und dennoch werden ihre biometrischen Daten durch die nachträgliche Fernidentifizierung ausgewertet.

b) Vergleich mit der Rasterfahndung

Das BVerfG hat sich noch in einem weiteren Verfahren mit den spezifischen Anforderungen an die massenweise Datenverarbeitung befasst. In dem Rechtsstreit um das SOG Mecklenburg-Vorpommern ging es nicht um die automatische Analyse vorhandener Daten, sondern um das Modell der Rasterfahndung, also um die Herausgabe von Daten aus behördlichen und privaten Verzeichnissen über eine Vielzahl von Personen nach Maßgabe von bestimmten Kriterien und deren nachträgliche Zusammenführung (vgl. dazu § 44 Abs. 1 SOG M-V; BVerfGE 165, 1).

Für das Verfassungsgericht wiegt bei der Rasterfahndung besonders schwer, dass keine hinreichende Nähebeziehung zwischen dem gefährdeten Rechtsgut und den vom Grundrechtsreingriff Betroffenen besteht (BVerfGE 165, 1 (97) Rn. 190).

Beide Formen der Fernidentifizierung setzen ebenso wie die Rasterfahndung voraus, dass bestimmte Informationen über die gesuchte Person bekannt sind. Bei der Rasterfahndung können dies Daten wie Geschlecht oder das Alter sein. Bei einer Fernidentifizierung sind die biometrischen Daten der Ausgangspunkt. Sie werden dann wie ein "Raster" über die Vergleichspersonen gelegt. Sowohl bei der Rasterfahndung als auch bei der Fernidentifizierung werden die Merkmale der gesuchten Person mit dem vollständigen verfügbaren Datenbestand abgeglichen. Im Unterschied zur Rasterfahndung kommt bei der Fernidentifizierung aber gegebenenfalls künstliche Intelligenz zum Einsatz.

Die Verwendung selbstlernender (KI-)Systeme begründet eine gesteigerte Eingriffsintensität. Die vom BVerfG bei der Datenanalyse mittels KI angeführten typischen Risiken eines „predictive policing“ bestehen bei der Fernidentifizierung zwar nicht (vgl. BVerfGE 165, 363 (408) Rn. 100). Jedoch gilt auch hier, dass durch die selbstlernenden Fähigkeiten einer künstlichen Intelligenz die staatliche Kontrolle und Nachvollziehbarkeit eingeschränkt sein kann (BVerfGE 165, 363 (408) Rn. 100). Auch kann es bei der Verwendung von Software privater Akteure und anderer Staaten zu einem Datenabfluss kommen (BVerfGE 165, 363 (408) Rn. 100), zumal die Anbieter in vielen Fällen nicht innerhalb der EU sitzen (vgl. kritisch daher Zöller, ZRP 2026, 128 (129)). All dies erhöht die Eingriffsschwere der Fernidentifizierung in die Grundrechte.

c) Kombination der verfassungsrechtlichen Anforderungen

Insgesamt sind aus diesen Gründen die Anforderungen an Eingriffe aus den Entscheidungen zur Rasterfahndung und automatisierter Datenverarbeitung kombiniert auf die Fälle der biometrischen Fernidentifizierung übertragbar (vgl. dazu auch Teichmann, NJOZ 2026, 705 (708); Coombe/Roth-Isigkeit, ZfDR 2024, 391 (413)). Das Verfahren ist nach verfassungsrechtlichen Maßstäben nur zulässig, wenn:

1. ein „besonders gewichtiges Rechtsgut“ geschützt wird (BVerfGE 165, 1 (90) Rn. 173; BVerfGE 165, 363 (410) Rn. 105; BVerfGE 141, 220 (303, 270) Rn. 207, 108) und dieses Schutzgut
2. einer „konkreten Gefahr“ ausgesetzt ist (BVerfGE 165, 1 (95) Rn. 185 ff.).

Das BVerfG zählt zu den „besonders gewichtigen Rechtsgütern“ insbesondere Leib, Leben, Freiheit der Person sowie Bestand oder Sicherheit des Bundes oder eines Landes (BVerfGE 165, 363 (410) Rn. 105).

d) Umsetzung in §§ 184b, 195b LVwG-E

Hinsichtlich der nachträglichen Fernidentifizierung in § 195b Abs. 1 LVwG-E erfüllt der Gesetzentwurf diese verfassungsrechtlichen Anforderungen. Bei den geschützten Rechtsgütern wird die Formulierung des BVerfG weitgehend übernommen und die „sexuelle Selbstbestimmung einer Person“ hinzugefügt. Diese Ergänzung ist angesichts des hohen Gewichts dieses Schutzguts und seiner Verankerung in Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG sehr gut nachvollziehbar und verfassungsrechtlich tragfähig.

Der Gesetzentwurf verlangt in § 195b LVwG-E als Gefahrenschwelle ferner eine konkrete Gefahr für die genannten Schutzgüter. Zwar ist als Tatbestandsvoraussetzung lediglich die „Gefahr“ normiert. Dies ist im Polizeirecht aber beim Fehlen anderer Anhaltspunkte als eine „konkrete Gefahr“ zu verstehen. Damit vollzieht der Gesetzentwurf die geforderte Gefahrenschwelle nach.

Die in § 184b Abs. 1 LVwG-E normierte Echtzeit-Fernidentifizierung verweist in Abs. 1 Satz 3 für die geschützten Rechtsgüter auf Art. 5 Abs. 1 UAbs. 1 lit. h) der KI-VO.

§ 184b Abs. 1 Satz 1 Nr. 1 LVwG-E verlangt damit eine Gefahr für Leben, Leib, Freiheit oder sexuelle Selbstbestimmung eines konkret bestimmten Opfers von Entführung, Menschenhandel oder sexueller Ausbeutung oder einer vermissten Person. Zusätzlich muss die Maßnahme der gezielten Suche nach diesen bestimmten Opfern bzw. der Suche nach Vermissten dienen.

§ 184 Abs. 1 Satz 1 Nr. 2 LVwG-E fordert das Abwenden einer konkreten, erheblichen und unmittelbaren Gefahr für das Leben oder die körperliche Unversehrtheit natürlicher Personen.

Auf Grund der fehlenden Normierung in Art. 5 Abs. 1 UAbs. 1 h) ii) Var. 1 KI-VO ist hier ein Vorgehen weder ausdrücklich zum Schutz der sexuellen Selbstbestimmung noch zum Schutze der Freiheit einer Person möglich.

§ 184 Abs. 1 Satz 1 Nr. 3 LVwG-E verlangt die Abwehr einer Gefahr für Leib, Leben oder Freiheit oder den Bestand oder die Sicherheit des Bundes oder eines Landes, die durch die Gefahr eines tatsächlichen und bestehenden oder tatsächlichen und vorhersehbaren Terroranschlags ausgelöst wird. Es bedarf somit erstens der Gefahr eines Terroranschlags und zweitens der Gefahr einer dadurch ausgelösten Rechtsgutsgefährdung.

Nicht ersichtlich ist, weshalb der Entwurf die Reihenfolge der geschützten Rechtsgüter im Vergleich zu § 184 Abs. 1 Satz 1 Nr. 1 LVwG-E verändert. Der Gesetzgeber sollte ferner erwägen auch in diesem Fall ein Vorgehen zum Schutz der sexuellen Selbstbestimmung zu erlauben.

Auch wenn es unrealistisch erscheint, dass ein Terrorangriff allein die sexuelle Selbstbestimmung gefährdet, würde die Aufnahme dieses Schutzguts das Interesse des Gesetzgebers widerspiegeln, dieses den anderen besonders gewichtigen Rechtsgütern umfassend gleichzustellen.

Hinsichtlich der Gefahrenschwelle erfordern alle Varianten der Echtzeit-Fernidentifizierung eine „Gefahr“. Damit ist im Sprachgebrauch des deutschen Gefahrenabwehrrechts bei Fehlen einer Präzisierung regelmäßig die konkrete Gefahr gemeint. Die Eingriffsschwellen entsprechen damit grundsätzlich den verfassungsrechtlichen Anforderungen. Des Weiteren sind die Voraussetzungen an die zu schützenden Rechtsgüter eingehalten.

Die biometrische Fernidentifizierung geht allerdings in einem besonderen Punkt über die Eingriffstiefe durch Rasterfahndung und automatischen Datenabgleich hinaus. Die enorm große Zahl an unbeteiligten Personen, deren biometrische Daten verarbeitet werden, verstärkt die Grundrechtsbeeinträchtigung (vgl. BVerfGE 115, 320 (357)) und kann „chilling effects“ auslösen (vgl. EG. 32 KI-VO). Durch die permanente Observation des öffentlichen Raumes (Echtzeit) und des Internets (nachträglich) kann bei Menschen ein besonderes Gefühl des Beobachtet-Seins entstehen. Wer dauerhaft damit rechnen muss, durch Gefahrenabwehrbehörden identifiziert zu werden, passt sein Verhalten möglicherweise unbewusst an, auch wenn er selbst für polizeiliches Einschreiten überhaupt keinen Anlass bietet. Das Wissen um die dauerhafte Möglichkeit der automatischen Identifizierung anhand biometrischer unveränderlicher Merkmale wiegt dabei noch schwerer als das bloße Beobachtetwerden, das schon mit der klassischen, linearen Videoüberwachung eintritt (§ 184 Abs. 2 LVwG). Die Ausübung grundrechtlicher Freiheit würde so gefährdet (Zöller, ZRP 2026, 128 (129)).

Aus diesem Grund könnte man erwägen, die Voraussetzungen der biometrischen Fernidentifizierung noch weiter anzuheben. Das BVerfG hat über diese Frage bisher nicht entschieden. Es wäre aber denkbar, dass bei gegebenem Anlass aus den betroffenen Grundrechten gerade wegen der umfassenden „chilling effects“ noch anspruchsvollere Eingriffshürden hergeleitet werden.

Der Entwurf für die §§ 184b, 195b LVwG wäre jedenfalls dann auf der sicheren Seite, wenn man die Eingriffsschwelle von einer lediglich konkreten Gefahr auf eine „dringende Gefahr“ hochstuft.

2. Unionsrechtliche Rahmenbedingungen: KI-Verordnung

Der europäische Gesetzgeber hat mit der sog. KI-VO besondere Anforderungen für den Einsatz von künstlicher Intelligenz normiert und bestimmte Praktiken der KI-Nutzung mit einem generellen Verbot belegt. Während die Vorgaben für die biometrische Echtzeit-Fernidentifikation

sehr ausführlich normiert sind (a)), hält sich der Unionsgesetzgeber bei den Anforderungen an nachträgliche biometrische Fernidentifizierung zurück (b)).

a) Biometrische Echtzeit-Fernidentifikation

Art. 5 Abs. 1 UAbs. 1 lit. h) KI-VO verbietet die Verwendung von biometrischen Echtzeit-Fernidentifizierungssystemen in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken. Mit „Strafverfolgungszwecken“ ist nach Art. 3 Nr. 46 KI-VO auch präventives Polizeihandeln, also Gefahrenabwehr gemeint. In anderen Sprachfassungen tritt das deutlicher zutage, wenn etwa die englische Version der KI-VO an dieser Stelle von „law enforcement“ spricht. Auch im Spanischen und Französischen („garantía del cumplimiento del Derecho“; „fins répressives“) lassen sich keine Beschränkungen auf Zwecke der Strafverfolgung finden.

aa) Unbedingte Erforderlichkeit zur Erreichung spezifischer Ziele

(1) Vorgaben

Nach den Ausnahmenvorschriften des Art. 5 Abs. 1 UAbs. 1 lit. h) i) - iii) KI-VO ist die KI-gestützte Fernidentifizierung nur zulässig, soweit sie „unbedingt erforderlich“ ist, um eines der genannten Ziele zu erreichen. Sie ist nur in drei Fällen gestattet:

1. Sie ist unbedingt erforderlich, um vermisste Personen oder Opfer von Entführung, Menschenhandel oder sexueller Ausbeutung zu suchen.
2. Sie ist unbedingt erforderlich, um konkrete, erhebliche und unmittelbare Gefahren für das Leben oder die körperliche Unversehrtheit oder eine tatsächliche und bestehende oder tatsächliche und vorhersehbare Gefahr eines Terroranschlags abzuwenden.
3. Sie ist unbedingt erforderlich, um eine Person aufzuspüren, die der Begehung einer Straftat verdächtigt wird sowie für strafrechtliche Ermittlungen und Strafverfahren bei Straftaten mit einer Höchststrafe von vier oder mehr Jahren.

Die dritte Variante ist für den Bereich der Gefahrenabwehr nicht von Bedeutung; hier geht es tatsächlich um Strafverfolgung im engeren Sinne.

Die unbedingte Erforderlichkeit wird in der KI-VO nicht ausdrücklich definiert. Allerdings lassen sich Art. 5 Abs. 3 UAbs. 2 S. 1 KI-VO genauere Hinweise entnehmen. Diese Vorschrift regelt nämlich, wann die zuständige Justizbehörde (damit wird auch ein Richtervorbehalt ermöglicht) die Genehmigung für die Durchführung einer Echtzeit-Fernidentifizierung erteilen darf.

Das ist nur der Fall, „wenn sie auf der Grundlage objektiver Nachweise oder eindeutiger Hinweise, die ihr vorgelegt werden, davon überzeugt ist, dass die Verwendung des betreffenden biometrischen Echtzeit-Fernidentifizierungssystems für das Erreichen eines der in Absatz 1 Unterabsatz 1 Buchstabe h) genannten Ziele — wie im Antrag angegeben — notwendig und verhältnismäßig ist und insbesondere auf das in Bezug auf den Zeitraum sowie den geografischen und persönlichen Anwendungsbereich unbedingt erforderliche Maß beschränkt bleibt.“

Die Anwendung der Echtzeit-Fernidentifizierung wird damit an einen besonders strengen Verhältnismäßigkeitsmaßstab gekoppelt. Weniger eingriffsintensive Standardmaßnahmen können also vorrangig sein (vgl. auch Schäfer-Lässig, GSZ 2026, 31 (33); BeckOK KI-Recht/Raue, 7. Ed. 1.8.2026, KI-VO Art. 5 Rn. 193). Zudem muss die Fernidentifizierung auch räumlich, zeitlich sowie in Bezug auf den erfassten Personenkreis möglichst beschränkt bleiben. Weil die „unbedingte Erforderlichkeit“ auch schon in Art. 5 Abs. 1 UAbs. 1 lit. h) KI-VO normiert ist, muss sie sich auch auf Tatbestandsebene in den mitgliedstaatlichen Normen wiederfinden.

(2) Umsetzung

§ 184b LVwG-E setzt die Vorgaben der unionsrechtlichen Ausnahmegesetzgebung nahezu wortlautgetreu um. Der Vorschrift liegt erkennbar die Absicht zugrunde, die Voraussetzungen aus der Rechtsprechung des BVerfG einerseits und die unionsrechtlichen Voraussetzungen andererseits abzubilden. § 184b Abs. 1 Nr. 1 LVwG-E adressiert das Ziel, vermisste Personen und Opfer von bestimmten Straftaten zu finden und verbindet dieses mit den verfassungsrechtlich vorgezeichneten Rechtsgütern. Nr. 2 nimmt nur auf die unionsrechtliche Norm des Art. 5 Abs. 1 UAbs. 1 lit. h) ii) Alt. 1 KI-VO Bezug, weil dort bereits die zu schützenden Rechtsgüter Leben und körperliche Unversehrtheit aufgeführt sind. Das führt freilich dazu, dass eine Fernidentifizierung bei Gefahren, die nur Freiheit oder sexuelle Selbstbestimmung betreffen, ohne zugleich die körperliche Unversehrtheit zu beeinträchtigen, nicht zulässig ist. Andersherum wird bei § 184b Abs. 1 Nr. 3 LVwG-E die unionsrechtliche Ausnahmegesetzgebung der Terrorgefahr durch die Gefahr für Leib, Leben oder Freiheit ergänzt, während das Unionsrecht es bei einem „Terroranschlag“ belässt.

Der Gesetzentwurf versucht also allenthalben die unions- und die verfassungsrechtlichen Anforderungen nebeneinander abzudecken und dabei nach dem Prinzip der höchsten Eingriffsschwelle diejenigen Aspekte des nationalen Rechts oder Unionsrechts explizit hinzuzufügen, die über die jeweils andere Rechtsordnung hinausgehen (Drs. 20/4284, S. 46).

Typischerweise wird es zwischen den unionsrechtlich motivierten Voraussetzungen und denjenigen, die sich aus dem mitgliedstaatlichen Verfassungsrecht ergeben, Überschneidungen geben. So sind etwa kaum Fälle denkbar, in denen Terroranschläge sich gegen etwas anderes

richten als gegen Leib, Leben, Freiheit oder Bestand und Sicherheit des Bundes oder eines Landes. Die Vorschrift wird dadurch einerseits schwer lesbar und enthält tatbestandliche Dopplungen, gewährleistet aber andererseits auch die kumulative Erfüllung von Anforderungen aus dem Unions- und Verfassungsrecht.

Die Formulierung „unbedingt erforderlich“ wurde in den § 184b Abs. 1 S. 3 LVwG-E übernommen und hat ihren Ursprung ebenfalls in Art. 5 Abs. 1 UAbs. 1 lit. h) KI-VO. Ein Verstoß gegen das Normwiederholungsverbot (Pechstein/Nowak/Häde, Frankfurter Kommentar EUV/GRC/AEUV/Gundel, 2. Aufl. 2023, AEUV Art. 288 Rn. 10) ist in diesem Zusammenhang nicht zu befürchten, weil der unionsrechtliche Hintergrund der Vorschrift sich insgesamt aus den verschiedentlichen Verweisen auf die KI-VO hinreichend deutlich ergibt.

Die „unbedingte Erforderlichkeit“ ist dem deutschen Polizeirecht als Rechtsbegriff bisher weitgehend fremd (anders aber etwa die unionsrechtlich motivierte Vorschrift des § 48 Abs. 1 BDSG). Es wird sich demnach erst eine eigenständige Auslegung in Rechtsprechung und Praxis bilden müssen, die aber auf die unionsrechtlichen Hintergründe der Formulierung Bezug zu nehmen hat.

Der EuGH sieht in der unbedingten Erforderlichkeit an anderer Stelle „eine verschärfte Voraussetzung für die Rechtmäßigkeit der Verarbeitung solcher Daten, was u. a. bedeutet, dass die Einhaltung des Grundsatzes der „Datenminimierung“, wie er sich aus Art. 4 Abs. 1 Buchst. c der RL 2016/680 ergibt, der in diesem Erfordernis eine spezifische Anwendung auf die genannten sensiblen Daten erfährt, besonders streng kontrolliert werden muss“ (EuGH BeckRS 2024, 772 Rn. 48).

Letztlich muss dem Rechtsanwender klar sein, dass die biometrische Fernidentifizierung nur als ultima ratio in Betracht kommen kann, wenn andere Möglichkeiten der Identifizierung aussichtslos sind (vgl. im Datenschutzrecht BeckOK DatenschutzR/Albers/Schimke, 56. Ed. 1.2.2026, BDSG § 48 Rn. 26).

Wie weit der eigenständige Gehalt der unbedingten Erforderlichkeit gegenüber dem ohnehin anwendbaren Verhältnismäßigkeitsgrundsatz reichen kann, ist dabei noch nicht ganz absehbar. Die Formulierung signalisiert aber immerhin eine sehr strenge Verhältnismäßigkeitsprüfung, bei der auch der räumliche und zeitliche Umfang der Maßnahme sowie der Umfang der Drittbetroffenheit zu berücksichtigen sind. Die Aufnahme der Voraussetzung ist zudem unionsrechtlich geboten.

bb) Grundrechte-Folgenabschätzung und Registrierung des KI-Systems

Als zusätzliche Anforderung für eine biometrische Echtzeit-Fernidentifizierung nennt Art. 5 Abs. 2 UAbs. 2 S. 2 KI-VO die Durchführung einer Grundrechte-Folgenabschätzung nach Art. 27 KI-VO und die Registrierung des KI-Systems in einer EU-Datenbank nach Art. 49 KI-VO. § 184b Abs. 1 S. 4 LVwG-E vollzieht diese Anforderung nach, indem auf die Einhaltung des Art. 5 Abs. 2 KI-VO hingewiesen wird.

Aus der Gesetzesbegründung ergibt sich dann zweifelsfrei, dass die Grundrechte-Folgenabschätzung und die Registrierung des Systems mit dem Verweis zu Tatbestandsvoraussetzungen gemacht werden sollen (Drs. 20/4284, S. 45). Aus Gründen der Normenklarheit wäre es aber vorzugswürdig, wenn in der Ermächtigungsgrundlage des § 184b LVwG-E auf die Erforderlichkeit der Grundrechte-Folgenabschätzung nach Art. 27 KI-VO und auf die Registrierung nach Art. 49 KI-VO explizit hingewiesen würde.

b) Nachträgliche biometrische Fernidentifizierung

Für die nachträgliche Fernidentifizierung in § 195b LVwG-E enthält Art. 26 Abs. 10 KI-VO einige Vorgaben. Die negativ formulierte Zweckbindung aus Art. 26 Abs. 10 UAbs. 3 KI-VO belegt, dass eine nachträgliche biometrische Fernidentifizierung nicht nur im Rahmen der Strafverfolgung, sondern auch zur Gefahrenabwehr und zur Suche nach vermissten Personen zulässig sein kann. Von dieser Möglichkeit macht § 195b LVwG-E Gebrauch. § 195b Abs. 2 Satz 3 LVwG-E verweist zusätzlich auf die Anforderungen des Art. 26 Abs. 10 UAbs. 3 der KI-VO.

Die Pflicht zur Genehmigung einer nachträglichen biometrischen Fernidentifizierung nach Art. 26 Abs. 10 UAbs. 1 KI-VO durch eine Justizbehörde oder eine justiziell überprüfbare Verwaltungsbehörde betrifft nur Fälle, in denen eine Person der Begehung einer Straftat verdächtigt oder deswegen verurteilt wurde. Bei Gefahrenabwehrmaßnahmen ist die Genehmigung unionsrechtlich nicht verpflichtend (vgl. Martini/Wendehorst/Eisenberger/Binder, 2. Aufl. 2026, KI-VO Art. 26 Rn. 70). Indem § 195b Abs. 3 LVwG-E die nachträgliche Fernidentifizierung einem Richtervorbehalt unterstellt, geht der Gesetzentwurf zurecht über die niedrigen unionsrechtlichen Anforderungen hinaus und fördert dadurch den effektiven Grundrechtsschutz.

c) Verbot der Inbetriebnahme von Datenbanken zur Gesichtserkennung

Als weitere verbotene Praktik nennt Art. 5 Abs. 1 UAbs. 1 lit. e) KI-VO „das Inverkehrbringen, die Inbetriebnahme für diesen spezifischen Zweck oder die Verwendung von KI-Systemen, die Datenbanken zur Gesichtserkennung durch das ungezielte Auslesen von Gesichtsbildern aus dem Internet oder von Überwachungsaufnahmen erstellen oder erweitern.“ Anders als das

soeben behandelte Verbot nach Art. 5 Abs. 1 UAbs. 1 lit. h) KI-VO kennt diese Vorschrift keine Ausnahmetatbestände, die diese Maßnahme im Einzelfall erlauben könnten.

Allerdings handelt es sich bei der biometrischen Fernidentifizierung auch nicht um ein „ungezieltes“ Auslesen von Gesichtsbildern, sondern im Gegenteil um ein gezieltes, mit dem eine spezielle Person identifiziert werden soll (Leitlinien der Kommission zu verbotenen Praktiken der künstlichen Intelligenz, C (2025) 5052 final, Rn. 228 f.; BeckOK KI-Recht/Raue, 7. Ed. 1.8.2026, KI-VO Art. 5 Rn. 131). Das Verbot betrifft daher nicht die §§ 184b, 195b LVwG-E.

II. Rechtsstaatliche Rahmenbedingungen

1. Überblick

Die Normen des Gesetzentwurfs gewährleisten die Einhaltung rechtsstaatlich gebotener Rahmenbedingungen vorbehaltlich der nachfolgend genannten Punkte in ausreichendem Maße.

Nach der Rechtsprechung des BVerfG zur automatisierten Datenanalyse sind die rechtsstaatlichen Anforderungen variabel (BVerfGE 165, 363 (398) Rn. 71). Wie bereits herausgearbeitet, sind die Regelungen zur Echtzeit-Fernidentifizierung sowie zur nachträglichen Fernidentifizierung jeweils mit einem hohen Eingriffsgewicht verbunden, sodass die Anforderungen übertragbar sind (s.o. I. Allgemeine verfassungsrechtliche und unionsrechtliche Rahmenbedingungen).

Allgemeine rechtsstaatliche Hürden sind daher der Grundsatz der Verhältnismäßigkeit (BVerfGE 165, 363 (389) Rn. 51) sowie im Bereich der Datenverarbeitung die Grundsätze der Zweckbindung und Zweckänderung (BVerfGE 165, 363 (390) Rn. 55 ff.). Das BVerfG stellt weitergehend auf die Sicherung von Transparenz, das Vorhandensein von Rechtsschutz sowie auf sichtlicher Kontrolle (BVerfGE 165, 363 (398) Rn. 71) ab.

Gleichermaßen ergeben sich diese Anforderungen auch aus Art. 5 Abs. 1 UAbs. 1 lit. h), Abs. 2, Abs. 3 KI-VO. Diese Aspekte werden ausreichend in dem Regelungsentwurf berücksichtigt.

Die Regelungen bemühen sich eindeutig, den Grundsatz der Verhältnismäßigkeit zu wahren. So werden in § 184b Abs. 1 S. 3, 4 LVwG-E aufgrund der Eingriffsintensität strenge Verhältnismäßigkeitsmaßstäbe an die biometrische Echtzeit-Fernidentifizierung gestellt (s.o. I. 1. Biometrische Fernidentifizierung in der Rechtsprechung des BVerfG). Auch die zeitliche und örtliche Begrenzung der Maßnahme nach § 184b Abs. 2 LVwG-E dient der Wahrung des Verhältnismäßigkeitsgrundsatzes. Ähnliche Anhaltspunkte befinden sich für die nachträgliche Fernidentifizierung in § 195b Abs. 1 S. 4 LVwG-E, für den eine vergleichbar strenge Verhältnismäßigkeitsprüfung vorgesehen ist. In § 195b Abs. 2 S. 1 LVwG-E werden die legitimen Zwecke explizit und abschließend genannt.

Durch die strenge Verhältnismäßigkeitsprüfung können die einzelnen Maßnahmen nur in äußerst eingegrenzten Fällen zum Schutz von Rechtsgütern von besonderem Rang eingesetzt werden. Auch die zeitliche Begrenzung der Fernidentifizierung schwächt die Eingriffsintensität ab. Insgesamt bewirken die vorgesehenen Einschränkungen der Maßnahmen, dass der Eingriff auf das notwendige Minimum beschränkt ist.

Ein weiteres Kernelement der rechtsstaatlichen Ausgestaltung von heimlichen Maßnahmen ist die Transparenz gegenüber dem Betroffenen, die als nachträgliche Pflicht eingeführt wird. Die Benachrichtigungspflichten aus § 184c Abs. 2 S. 1 LVwG-E sowie § 195c Abs. 2 S. 1 LVwG-E zugunsten des Betroffenen einer Fernidentifizierung gewährleisten die Kenntnismahme und ermöglichen dadurch erst den Rechtsschutz. Unbeteiligte Dritte, die von der Streubreite der Maßnahme betroffen sind, werden allerdings nicht benachrichtigt. Dies sollte ausdrücklich gerechtfertigt werden. Begründet werden kann dies damit, dass sich durch eine Benachrichtigung der Eingriff vertiefen würde.

In beiden Maßnahmen ist die Benachrichtigung eine ausdrückliche und zwingende Voraussetzung für die Durchführung. Auch die jeweils vorgesehene zeitliche Zurückstellung zum Schutz des Zwecks der Datenerhebung ist dabei nicht zu beanstanden. Die Eingriffsvoraussetzungen sind jeweils hoch, sodass nur aufgrund der Gefahrenabwehr für die genannten gewichtigen Rechtsgüter überhaupt eingeschritten werden darf (s.o. I. Allgemeine verfassungsrechtliche und unionsrechtliche Rahmenbedingungen).

Eine verfrühte Mitteilung kann dabei die Maßnahme erschweren oder sie sogar unmöglich machen, sodass die effektive Gefahrenabwehr nicht gesichert wäre. Außerdem ermöglicht der nachträgliche Rechtsschutz eine Kontrolle und gegebenenfalls Entschädigung auf Sekundärebene.

Darüber hinaus wird die Transparenz auch durch die Zugangsbeschränkungen und -kontrollen sowie Protokollierungspflichten (dazu s.u. II. 2. Berichts- und Protokollierungspflichten) in § 184c Abs. 3 LVwG-E und in § 195c Abs. 3 LVwG-E gewährleistet. Nur eine begrenzte Anzahl qualifizierter Beschäftigter der Polizei (s.u. VI. Überprüfung der Ergebnisse) dürfen die Anwendung durchführen. Dadurch ist die Maßnahme genau nachvollzieh- und überprüfbar. Dies gewährleistet die Kontrolle durch Aufsicht und gleichermaßen den effektiven Rechtsschutz.

Ferner sind Regelungen zur Gewährleistung der Grundsätze der Zweckbindung und -änderung beim Umgang mit den biometrischen Daten vorgesehen (§ 184c Abs. 1 S. 1, 3 ff. LVwG-E sowie § 195c Abs. 1 S. 1, S. 3 ff. LVwG-E). Explizit dürfen diese Daten ausschließlich für den Zweck und den Sachverhalt verarbeitet werden, für den sie erhoben wurden. Nach Abschluss

der Überprüfung möglicher weiterer Maßnahmen sind die Daten grundsätzlich zu löschen. Nur im Falle weiterer polizeilicher Maßnahmen dürfen sie gespeichert werden. Insoweit entspricht dies den Anforderungen, die das BVerfG aufgestellt hat. Aufgrund des Ausschlusses der Zweckänderung und jeglicher weiterer Nutzung nach § 188a Abs. 1, 2 LVwG ist die strenge Zweckbindung im notwendigen Umfang gewahrt.

Die Regelungen verweisen auch auf den erforderlichen Rechtsschutz. Über § 184c Abs. 2 S. 2 LVwG-E und § 195c Abs. 2 S. 2 LVwG-E ist nach § 186 Abs. 7 S. 3 LVwG auf den Rechtsschutz hinzuweisen. Damit ist dem Betroffenen zumindest nach der Maßnahme die gerichtliche Kontrolle bekannt. Dies genügt, um die Rechtsschutzmöglichkeit nach Art. 19 Abs. 4 GG in rechtsstaatlich gebotener Weise sicherzustellen. Dies wird auch durch die Berichts- und Protokollpflichten effektuert.

In den Regelungen ist ferner eine gerichtliche Anordnung der Maßnahme vorgesehen (vgl. § 184b Abs. 3, 4 LVwG-E, § 195b Abs. 3 LVwG-E). Die richterliche Anordnung nach § 184b Abs. 3 LVwG-E sowie § 195b Abs. 3 S. 1 LVwG-E soll grundsätzlich vorab erfolgen. Dies kann jedoch (im Falle des § 184b Abs. 3 LVwG-E nur unverzüglich) nachgeholt werden, sofern das Einholen aufgrund von Gefahr im Verzug nicht möglich war. Die mögliche Wiederholung der Maßnahme nach Fristablauf gemäß § 184b Abs. 3 S. 3 LVwG-E und die Unterrichtungspflicht gemäß § 195b Abs. 3 S. 2 LVwG-E in Verbindung mit § 186 Abs. 4 LVwG ermöglichen eine stetige Kontrolle des Gerichts über die eingriffsintensive Maßnahme. Durch die gerichtliche Anordnung heimlicher Maßnahmen wird der Rechtsschutzgarantie des Betroffenen nach Art. 19 Abs. 4 GG Rechnung getragen (Heusch/Ullrich/Posser, HdB d. VerfR in d. Praxis/Braun, 1. Aufl. 2024, § 7 Rn. 92).

Auf diese Weise sind die hohen Eingriffsvoraussetzungen grundsätzlich im Vorwege überprüft und werden bei Aufrechterhaltung gerichtlich weiter kontrolliert. Dadurch gewährleistet der Regelungsentwurf die Einhaltung der Rechtsschutzgarantie nach Art. 19 Abs. 4 GG.

Zudem ist die notwendige aufsichtliche Kontrolle in § 184c Abs. 3 S. 2 LVwG-E sowie § 195c Abs. 3 S. 2 LVwG-E vorgesehen. Der Entwurf gewährleistet über den Verweis auf § 186c LVwG die Kontrolle durch die Landesbeauftragte für Datenschutz nach § 186b LVwG.

Die gerichtliche Anordnung ist nur auf Antrag der Leiterin oder des Leiters des Landespolizeiamtes, des Landeskriminalamtes, einer Polizeidirektion oder durch von ihr oder ihm besonders beauftragte Personen des Polizeivollzugsdienstes möglich (vgl. § 184b Abs. 3 S. 1 LVwG-E, § 195b Abs. 3 S. 1 LVwG-E). Diese begrenzte Zuständigkeit beschränkt die Antragsmöglichkeit auf eine geringe Anzahl an Personen. Dazu kommt, dass sich ohnehin nur in begrenzten Fällen mit der Möglichkeit der Maßnahme auseinandergesetzt werden kann. Dadurch wird dem

hohen Eingriffsgewicht und der besonderen Gefahrenlage, die für das Beantragen der Maßnahme vorausgesetzt ist, Rechnung getragen (siehe zur Rasterfahndung PdK SH/Martens, LVwG § 195a).

Damit sind nicht nur die nach der Rechtsprechung des BVerfG sowie nach der KI-VO erforderlichen, sondern auch weitergehende Mechanismen als rechtsstaatliche Hürden errichtet.

2. Berichts- und Protokollierungspflichten

a) Berichtspflichten

Über die Protokollierungspflicht ist die Landesbeauftragte für Datenschutz zur Kontrolle gehalten und die Landesregierung muss den Landtag unterrichten (vgl. § 186b Abs. 2 LVwG). Die Aufnahme der neuen Maßnahmen in § 186c LVwG ist insoweit sinnvoll, da eine wirksame rechtsstaatliche Kontrolle das Bereitstellen der notwendigen Informationen voraussetzt (Dürrig/Herzog/Scholz/Schwarz, 110. EL Stand März 2026, GG Art. 38 Rn. 287).

Aufgrund der Berichtspflicht über die erfolgten heimlichen und damit eingriffsintensiven Maßnahmen kann der Landtag das tatsächliche Ausmaß der Regelung kontrollieren. Gerade die Mitteilung über das Ergebnis der Maßnahme ermöglicht nicht nur die Überprüfung der Wirksamkeit, sondern auch der Fehleranfälligkeit des Systems. Die gewählte Zeitabfolge von jährlichen Berichten genügt, weil die Eingriffsvoraussetzungen hoch sind und es erwartungsgemäß nicht zu einer Vielzahl von Maßnahmen zur Fernidentifizierung kommen wird. Auf diese Weise können etwaige Fehlentwicklungen rechtzeitig abgeschätzt werden.

b) Protokollierungspflichten

Die vorgesehenen Protokollierungspflichten überzeugen aufgrund ihrer Zweckmäßigkeit zur Gewährleistung von Transparenz und wirksamer gerichtlicher Kontrolle der Maßnahme (Heusch/Ullrich/Posser, HdB d. VerfR in d. Praxis/Braun, 1. Aufl. 2024, § 7 Rn. 92).

Grundsätzlich sind nach § 186c Abs. 1 LVwG das eingesetzte Mittel, der Zeitraum des Einsatzes, Angaben, die die Feststellung der erhobenen Daten ermöglichen, und die durchführende Organisationseinheit zu protokollieren. Dies wird durch § 184c Abs. 3 S. 2 LVwG-E leicht erweitert, der auch die Art der automatisierten Anwendung und die Angabe der Beschäftigten der Polizei bei der Protokollierung fordert. Dadurch können das eingesetzte System und die Anwender nachvollzogen und in die Überprüfung einbezogen werden. Die detaillierte Dokumentation dient der Aufsicht nach § 186b LVwG und der gerichtlichen Kontrolle. Der Wortlaut des § 186c Abs. 1 Nr. 2 LVwG könnte jedoch konkreter sein. Um die Transparenz zu stärken,

sollte hier nicht nur ungenau formuliert der „Zeitraum des Einsatzes“ genannt werden. Im Rahmen der Abfrage konkreter Bilder in Echtzeit sollte der Zeitpunkt exakt benannt sein, um die Streubreite, gerade hinsichtlich der Betroffenheit möglicher unbeteiligter Dritter, nachverfolgen zu können. Zumindest sollte der Zeitraum gesetzlich genauer konkretisiert werden. An dieser Stelle wären demnach das Datum sowie die sekundengenaue Angabe des Beginns und des Endes der Maßnahme überzeugender. Die Spezifizierung der Protokollierungspflichten („sekundengenau“) kann ebenso in § 184c Abs. 3 S. 2 LVwG-E aufgenommen werden, wenn sie sich nur auf die Echtzeit-Fernidentifizierung beziehen soll. Sinnvoll wäre es ferner, den überprüften örtlichen Raum anzugeben, um die Streubreite der Maßnahme zu überblicken und die Eingriffsintensität nachzuvollziehen. Dies kann etwaige Abwägungen oder Schlussfolgerungen für den Einsatz der Fernidentifizierung beeinflussen.

III. Unterscheidung der rechtlichen Anforderungen an eine Echtzeit-Fernidentifizierung und an eine nachträgliche Fernidentifizierung

Der Gesetzentwurf trägt der gebotenen strengen Unterscheidung zwischen der Echtzeit-Fernidentifizierung und der nachträglichen Fernidentifizierung Rechnung.

Gemäß Art. 3 Nr. 42 KI-VO ist ein „biometrisches Echtzeit-Fernidentifizierungssystem“ ein biometrisches Fernidentifizierungssystem, bei dem die Erfassung biometrischer Daten, der Abgleich und die Identifizierung ohne erhebliche Verzögerung erfolgen, und das zur Vermeidung einer Umgehung der Vorschriften nicht nur die sofortige Identifizierung, sondern auch eine Identifizierung mit begrenzten kurzen Verzögerungen umfasst. Erforderlich für die Echtzeit-Fernidentifizierung ist dementsprechend „Live-Material oder Near-live-Material“, wie etwa Videoaufnahmen, die von einer Kamera erzeugt werden (vgl. Coombe/Roth-Isigkeit, ZfDR 2024, 391 (397)).

Hingegen ist gemäß Art. 3 Nr. 43 KI-VO ein „System zur nachträglichen biometrischen Fernidentifizierung“ ein biometrisches Fernidentifizierungssystem, das kein biometrisches Echtzeit-Fernidentifizierungssystem ist. Insofern ist bei der nachträglichen Fernidentifizierung die Erfassung der Daten und der Abgleich mit einer bestehenden biometrischen Datenbank zeitlich verzögert möglich und es können auch ältere Bild- oder Videoaufnahmen für eine biometrische Fernidentifizierung genutzt werden (Coombe/Roth-Isigkeit, ZfDR 2024, 391 (397)).

Nach dem Wortlaut könnten bereits kleinere Verzögerungen der Bildauswertung den (strengeren) Regulierungsbereich der Echtzeit-Fernidentifizierung umgehen. Deshalb ist eine zweckorientierte Gesamtbetrachtung erforderlich. Während Echtzeit-Systeme in der Regel dazu dienen, den aktuellen Aufenthaltsort einer gesuchten Person zu bestimmen, kommen nachträgliche

Systeme zum Einsatz, wenn zu zeigen ist, dass eine bestimmte Person, zu dem (in der Vergangenheit liegenden) Zeitpunkt der Bildaufnahme an einem bestimmten Ort gewesen ist (vgl. Coombe/Roth-Isigkeit, ZfDR 2024, 391 (397)).

Echtzeit-Fernidentifizierungen werden als KI-Systeme mit „unannehmbaren Risiken“ eingestuft und als verbotene Praktiken unter Art. 5 Abs. 1 KI-VO geführt. Sie können nur unter strengen materiellen und prozeduralen Voraussetzungen ausnahmsweise zur Strafverfolgung und damit auch zur Gefahrenabwehr in öffentlich zugänglichen Räumen eingesetzt werden (vgl. Coombe, GSZ 2024, 262 (263)). Der Einsatz von biometrischer Echtzeit-Fernidentifizierung ist nur in den von Art. 5 Abs. 1 UAbs. 1 lit. h), Abs. 2 bis 7 KI-VO aufgeführten Fällen zulässig (s.o. 2. Unionsrechtliche Rahmenbedingungen: KI-Verordnung).

Für die nachträgliche biometrische Fernidentifizierung werden bei den Betreiberpflichten für Hochrisiko-KI-Systeme in Art. 26 Abs. 10 KI-VO Sonderregelungen aufgestellt. Hieraus ergeben sich Anforderungen an die menschliche Aufsicht, Protokollierung und risikoadäquate Sicherung in organisatorischer Hinsicht (vgl. Teichmann, NJOZ 2026, 705 (707)). Dennoch weichen diese Sonderregelungen zum Teil erheblich von denen des Art. 5 Abs. 1 UAbs. 1 lit. h), Abs. 2 bis 7 KI-VO ab. So ist die Anwendung von Datensätzen nicht auf öffentlich zugängliche Räume beschränkt, es bedarf – anders als bei der Echtzeit-Fernidentifizierung – keiner unabhängigen Genehmigungsbehörde und die Beantragungsfrist ist deutlich großzügiger. Auch bestehen keine vergleichbaren Eingriffsschwellen in Art. 26 Abs. 10 KI-VO wie in Art. 5 Abs. 1 UAbs. 1 lit. h) KI-VO (vgl. Coombe, GSZ 2024, 262 (263)).

Insofern bestehen nach der KI-VO unterschiedliche rechtliche Anforderungen an eine Echtzeit-Identifizierung und eine nachträgliche Identifizierung.

Dennoch bestehen einige Gemeinsamkeiten zwischen der biometrischen Echtzeit-Fernidentifizierung und der nachträglichen Fernidentifizierung in Bezug auf die verfassungsrechtliche Bewertung. Mangels einer Vollharmonisierung bei den Regelungen ist hierbei vor allem auf das Grundgesetz abzustellen. Hierbei ist, wie bereits in den allgemeinen Ausführungen beschrieben, das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG betroffen (vgl. Coombe, GSZ 2024, 262 (264); s.o. I. Allgemeine verfassungsrechtliche und unionsrechtliche Rahmenbedingungen).

Für die verfassungsrechtliche Einordnung ist hierbei insbesondere das Urteil des Bundesverfassungsgerichts vom 16.02.2023 zur automatisierten Datenanalyse in Hamburg und Hessen maßgeblich (BVerfGE 165, 363; vgl. Teichmann, NJOZ 2026, 705 (708); s.o. I. Allgemeine verfassungsrechtliche und unionsrechtliche Rahmenbedingungen). Hiernach ist eine automatisierte Analyse und Auswertung polizeilich gespeicherter Daten nicht lediglich eine intensivere

Nutzung bereits vorhandener Informationen, sondern besitzt wegen der Möglichkeit, verborgene Zusammenhänge sichtbar zu machen und neues Wissen zu generieren, ein eigenständiges Eingriffsgewicht (vgl. Teichmann, NJOZ 2026, 705 (708)).

Die Grundrechtsbelastungen sind bei beiden Formen der Fernidentifizierung hoch. Teilweise wird sogar vertreten, dass die nachträgliche Fernidentifizierung noch etwas eingriffsintensiver ist (vgl. Coombe, GSZ 2024, 262, (262)). Eine hohe Eingriffsintensität besteht unter anderem aufgrund der Heimlichkeit der Maßnahme (zumindest bis zur nachträglichen Benachrichtigung der Betroffenen) und aufgrund von möglichen Einschüchterungseffekten, die sich durch das Wissen um oder die Befürchtung einer Datenerhebung ergeben (s.o. I. Allgemeine verfassungsrechtliche und unionsrechtliche Rahmenbedingungen).

Der Eingriff hinsichtlich der Datengrundlage ist unterschiedlich intensiv, denn je mehr Zeit zwischen Datenerfassung und biometrischer Identifizierung liegt, desto umfangreicher ist der mögliche Datenbestand, auf den zugegriffen werden kann. Insofern ist der Eingriff bei der nachträglichen biometrischen Identifizierung intensiver, denn es kann auf einen umfassenden Bestand an Daten zurückgegriffen werden (vgl. Coombe, GSZ 2024, 262 (265)).

Ein anderes Bild zeigt sich mit Blick auf die aufsichtliche Kontrolle und die Rechtsschutzmöglichkeiten der Betroffenen. Bei der Echtzeit-Identifizierung besteht für die Betroffenen aufgrund der fehlenden zeitlichen Unterbrechung keine Möglichkeit, die Identifizierungsmaßnahme durch ein Rechtsschutzverfahren zu verhindern. Dies gilt auch für die behördliche Kontrolle der Systeme. Bei der nachträglichen Identifizierung ist dieser Aspekt hingegen anders zu bewerten. Hier besteht deutlich mehr Zeit für aufsichtliche Kontrolle. Insofern ist die Eingriffsintensität für die nachträgliche Identifizierung hier etwas geringer zu bewerten (vgl. Coombe, GSZ 2024, 262 (265)). Vorbeugender Rechtsschutz ist aber auch bei der nachträglichen biometrischen Fernidentifizierung theoretisch möglich, in der Praxis aber schwierig zu erreichen.

Folglich handelt es sich sowohl bei der Echtzeit-Identifizierung als auch bei der nachträglichen Identifizierung um schwere Grundrechtseingriffe, die jeweils nur in engen Grenzen zulässig sind. Dennoch sind die Eingriffe unterschiedlich zu bewerten. Die entsprechende Unterscheidung zwischen den beiden Identifizierungsmaßnahmen nach der KI-VO ist dabei zulässig und ändert sich auch nicht im Lichte der Grundrechte.

Der vorliegende Entwurf trägt dieser Unterscheidung entsprechend Rechnung. Die §§ 184b und 184c LVwG-E zur Echtzeit-Fernidentifizierung beziehen sich direkt auf die Anforderungen aus Art. 5 KI-VO und die §§ 195b und 195c LVwG-E zur nachträglichen Identifizierung auf Art. 26 Abs. 10 KI-VO. Zu betonen ist, dass nach § 195b Abs. 1 S. 4 LVwG-E die nachträgliche

Fernidentifizierung nur zulässig ist, wenn sie für die Abwehr einer Gefahr für Leben, Leib, Freiheit oder die sexuelle Selbstbestimmung einer Person oder für den Bestand oder die Sicherheit des Bundes oder eines Landes unbedingt erforderlich ist und geht insofern sogar über die Anforderungen aus Art. 26 Abs. 10 KI-VO hinaus.

IV. Verfassungsrechtliche Erheblichkeit der Herkunft von Referenzdaten für Fernidentifizierungen

Die Frage der Herkunft von Referenzdaten aus einem geschlossenen, polizeilich vorgehaltenen Referenzbestand oder einem biometrischen Abgleich mit im Internet vorhandenen Bildern ist verfassungsrechtlich erheblich. Hierbei ist der Begriff der „Referenzdaten“ i.S.v. Art. 3 Nr. 41 KI-VO zu verstehen.

Bei bereits rechtmäßig in polizeilichen Systemen abgespeicherten Daten handelt es sich um einen geschlossenen, polizeilichen Referenzbestand. Hierbei besteht der Zugriff auf einen begrenzten Bestand bereits erhobener Daten, sodass der Eingriff lediglich in der erneuten Verwendung und automatisierten Auswertung der Daten liegt (vgl. Teichmann, NJOZ 2026, 705 (706)).

Hiervon unterscheidet sich der biometrische Abgleich mit vorhandenen Bildern aus dem Internet, bei dem gerade kein geschlossener Referenzbestand besteht, sondern auf einen offenen Datenraum zugegriffen wird (vgl. Teichmann, NJOZ 2026, 705 (706)).

Für die verfassungsrechtliche Einordnung ist das Urteil des BVerfG vom 16.02.2023 zur automatisierten Datenanalyse in Hamburg und Hessen auch hier maßgeblich (vgl. Teichmann, NJOZ 2026, 705 (708); BVerfGE 165, 363)).

In Bezug auf den Referenzbestand steigt die Eingriffsintensität, wenn offene und massenhafte Datenräume durchsucht werden. Bei einer internetbasierten Gesichtserkennung wird auf einen unbegrenzten Identifizierungsraum zurückgegriffen. Je tiefer und breiter die einbezogenen Datenbestände sind, desto strenger fallen die Anforderungen für die Rechtfertigung aus (vgl. Teichmann, NJOZ 2026, 705 (708)). Dem „Identifizierungsraum Internet“ kann sich in der heutigen Zeit faktisch kein Mensch entziehen. Insofern ist der Eingriff als besonders schwerwiegend zu bewerten und als schwerer als bei einer polizeilichen Datenbank.

Dieser Eingriff betrifft auch hier nicht nur die informationelle Selbstbestimmung, sondern auch die freiheitsichernde Funktion von Anonymität in Bezug auf das menschliche Verhalten.

Hieraus folgt nach der Rechtsprechung des Bundesverfassungsgerichts, dass es einer hinreichenden qualifizierten Ermächtigungsgrundlage bedarf, die Eingriffsschwellen, Zweckbindung, Datenkategorien und Kontrollmechanismen normiert. Diese Grundsätze sind in Bezug auf die biometrische Fernidentifizierung aufgrund der Eingriffstiefe sogar zu verschärfen und vom Gesetzgeber zu beachten (s.o. I. Allgemeine verfassungsrechtliche und unionsrechtliche Rahmenbedingungen). Hierbei ist zu berücksichtigen, dass bei Gesichtserkennung mit Daten gearbeitet wird, die körpernah und unveränderlich sind. Außerdem besteht die Gefahr, dass die Maßnahme eine Vielzahl unbeteiligter Personen erfasst oder mittelbar in den Referenzraum einbezieht (vgl. Teichmann, NJOZ 2026, 705 (706)).

In Bezug auf §§ 195b und 195c LVwG-E ist anzumerken, dass es sich um eine erforderliche eigenständige Eingriffsnorm handelt, die eine qualifizierte Ermächtigungsgrundlage darstellt, sich auf besonders schwerwiegende Gefahren bezieht, eine qualifizierte Erforderlichkeit verlangt, einer richterlichen Anordnung bedarf und Suchparameter begrenzt. Auch bestehen Benachrichtigungs- und Kontrollmechanismen. Insofern ist eine Begrenzung der Datenquellen für Referenzdaten auf öffentlich zugängliche Daten vorhanden, Echtzeit-Übertragungen sind ausgeschlossen und der Kernbereichsschutz ist gewährleistet. Weitere Einschränkungen sind bisher nicht vorgesehen.

Darüber hinaus sind die Hürden in §§ 195b und 195c LVwG-E deutlich höher als nach § 195 Abs. 2 LVwG-E, der sich lediglich auf den Abgleich mit polizeilichen Datenbanken bezieht. Insofern wird der notwendigen Differenzierung hier Rechnung getragen. Redaktionell sei hier darauf verwiesen, dass § 195 Abs. 2 S. 2 lit. b LVwG-E auf „eine Gefahr im Sinne der Nummer 1“ verweist, obwohl der Satz mit Buchstaben gegliedert ist. Darüber hinaus sei angemerkt, dass die Verweisung in § 195 Abs. 2 S. 5 LVwG-E auf § 195c Abs. 3 LVwG-E insofern unklar ist, als dass der Verweis auf die Protokollpflichten ins Leere läuft. § 186c LVwG-E enthält keinen Verweis auf § 195 LVwG-E.

V. Zeitliche Höchstdauer der Maßnahme und Befristung für Fernidentifizierungen

Das Absehen von einer zeitlichen Höchstdauer der Maßnahme in § 184b LVwG-E überzeugt in der Kombination mit der Befristung der Maßnahme auf maximal sieben Tage pro Genehmigung. Die Regelung in § 184b Abs. 3 S. 2 f. LVwG-E setzt durch das Vorsehen der Befristung auf maximal sieben Tage ohne eine Gesamthöchstdauer die Vorgaben des Art. 5 Abs. 2 UAbs. 2 S. 1, Abs. 3 UAbs. 2 S. 2 KI-VO um. Dies ist nach Art. 5 Abs. 5 KI-VO entsprechend möglich. Art. 5 Abs. 2 UAbs. 2 S. 1 KI-VO verlangt ausdrücklich, „notwendige und verhältnismäßige Schutzvorkehrungen und Bedingungen“, „insbesondere in Bezug auf die zeitlichen, geografischen und personenbezogenen Beschränkungen“ vorzusehen. Weitergehend wird dies in Art. 5 Abs. 3 UAbs. 2 KI-VO für die richterliche Genehmigung verschärft. Diese darf nur erteilt

werden, wenn die Verwendung „auf das in Bezug auf den Zeitraum sowie den geografischen und persönlichen Anwendungsbereich unbedingt erforderliche Maß beschränkt bleibt.“ Eine Höchstdauer der Maßnahme sowie eine Befristung sind darin nicht konkret vorgegeben, aber die nationale Umsetzung muss den Anforderungen des Art. 5 Abs. 1 UAbs. 1 lit. h), Abs. 2, Abs. 3 KI-VO entsprechen. Eine zeitliche Schutzmaßnahme ist daher erforderlich.

Diesen Anforderungen des Unionsrechts wird die Maßnahme gerecht. Eine Maßnahme ohne eine zeitliche Höchstdauer wirkt aus rechtsstaatlicher und unionsrechtlicher Perspektive zunächst bedenklich, da eine dauerhafte Echtzeit-Fernidentifizierung möglich wird. Damit einher gehen intensive Grundrechtseingriffe über einen potentiell langen und sogar unbegrenzten Zeitraum. Jedoch ist das Absehen von einer zeitlichen Höchstdauer der Maßnahme angesichts der hohen Eingriffsvoraussetzungen des § 184b LVwG-E zur effektiven Gefahrenabwehr sogar notwendig. Nur eine flexible Handhabung kann dem effektiven Schutz der Rechtsgüter des § 184b Abs. 1 LVwG-E gerecht werden. Gerade die bestimmten Ziele, die eine längere Maßnahme erforderlich machen, wären sonst unterlaufen. Dies betrifft beispielsweise die Suche nach bestimmten Opfern von Entführungen nach Art. 5 Abs. 1 UAbs. 1 lit. h) KI-VO. Einer ausufernden Grundrechtsbeeinträchtigung wirkt die grundsätzlich bestehende gerichtliche Kontrollinstanz vor der ersten Anordnung sowie vor einer Verlängerung entgegen. Diese ist jeweils erneut zu begründen und das Gericht prüft das Vorliegen der hohen Eingriffsvoraussetzungen, ohne dass sich die Begründungsanforderungen verändern (vgl. für den Prüfungsmaßstab der Verlängerung § 184b Abs. 3 S. 3 f. LVwG-E). Das Gewicht des Eingriffs in die Grundrechte der Betroffenen steigt zudem mit jeder weiteren Verlängerung der Maßnahme. Dadurch steigen ebenso die Anforderungen in der Verhältnismäßigkeitsprüfung in der gerichtlichen Abwägung. Die Grundrechte werden dann durch die stetige Kontrolle und die ansteigenden Rechtfertigungsanforderungen ausreichend berücksichtigt, während der Polizei dennoch eine flexible und vor allem effektive Gefahrenabwehr ermöglicht wird. Durch eben diese stetige Kontrolle ist eine effektive Schutzvorkehrung gewährleistet, welche die zeitliche Dauer auf das unbedingt erforderliche Maß beschränkt. Daher ist die zeitliche Länge von sieben Tagen zur Abwendung einer Gefahr für die in § 184b Abs. 1 LVwG-E aufgeführten Rechtsgüter sachgerecht.

VI. Überprüfung der Ergebnisse

Ausdrückliches Ziel der Prüfung durch „zwei qualifizierte Beschäftigte der Polizei“ (§ 184c Abs. 1 S. 2 LVwG-E) ist es, dass nur entsprechend ausgebildetes Personal die Ergebnisse des Abgleichs überprüft. Die gewählte Formulierung gewährleistet aber keine Qualitätssicherung.

Durch die vorausgesetzte Beschäftigung bei der Polizei ist ein Outsourcing an private Dienstleister und Verwaltungshelfer nicht möglich. Zu beachten ist, dass bestimmte Aufgaben nach

dem Funktionsvorbehalt des Berufsbeamtentums (Art. 33 Abs. 4 GG) von Beamten aufgrund des besonderen Dienst- und Treuverhältnisses auszuüben sind. Dennoch überzeugt die Voraussetzung, dass „Beschäftigte der Polizei“ das Ergebnis überprüfen. Die Tätigkeit bezieht sich allein auf das Überprüfen und Bestätigen des Ergebnisses. Im Vordergrund stehen das Nachvollziehen und Abgleichen des Ergebnisses. Diese Bestätigung muss einem Polizeivollzugsbeamten vorgelegt werden, bevor weitere polizeiliche Maßnahmen vorgenommen werden können. Dadurch liegt die Ausübung weiterer staatlicher Maßnahmen in der Hand von besonders verpflichteten Berufsbeamten. Damit ist es nicht zwingend erforderlich, dass es sich beim bloßen Abgleich um Polizeivollzugsbeamte handelt.

Allerdings wirft das Merkmal der Qualifikation der Beschäftigten Bedenken auf. Auf Grundlage dieser Bestätigung können weitere Maßnahmen getroffen werden, sodass die Gewährleistung der Qualifikation von elementarer Bedeutung ist.

Dies ist weiter konkretisierungsbedürftig. Ein Ansatz wäre es, für das Bestimmen auf die Anforderungen von Art. 14 Abs. 5 UAbs. 1 KI-VO oder Art. 26 Abs. 2 KI-VO abzustellen. Diese stellen auf die „erforderliche Kompetenz“ und „Ausbildung“ ab. Etwas weiter konkretisiert werden diese Angaben in den Erwägungsgründen zur KI-VO. In EG 73 S. 3 und EG 91 S. 3 der KI-VO wird für die Qualifikation zur Aufsicht auf eine (KI-)Kompetenz und eine Schulung abgestellt. Eine derartige Formulierung sollte im Gesetz aufgenommen werden, aber konkretisiert die „Qualifikation“ auch nicht vollständig. Es müssen letztlich in der praktischen Umsetzung klare Vorgaben für die „Qualifikation“ vorgesehen werden, um für die Aufsicht essentielle rechtliche, informationstechnische und forensische Fähigkeiten bei der Aufsicht sicherzustellen. In rechtlicher Hinsicht wären der datenschutzkonforme Umgang mit den Ergebnissen sowie die Fähigkeit, die Tragweite der Bestätigung durch eingriffsintensive Folgemaßnahmen einzuschätzen, notwendig. Informationstechnische Kenntnisse sind für das Nachvollziehen des technischen Vorgangs beispielsweise zur Fehlererkennung erforderlich. Da die Überprüfung des Ergebnisses eines Bildabgleichs ein forensischer Vorgang ist, müssen die Beschäftigten auch in diesem Aspekt qualifiziert sein.

Angemerkt sei allerdings, dass § 195c LVwG-E hinsichtlich der Überprüfung widersprüchlich erscheint. § 195c Abs. 1 S. 2 LVwG-E fordert die Auswertung nur durch „zwei Beschäftigte der Polizei“ während § 195c Abs. 3 S. 1 LVwG-E für den bloßen Systemzugang „qualifizierte Beschäftigte der Polizei“ voraussetzt. Angesichts der möglichen weiteren polizeilichen Maßnahmen, die gemäß § 195c Abs. 1 S. 2 LVwG-E nach der Auswertung erfolgen können, überzeugt dies nicht. Auch der strukturelle Vergleich zu § 184c Abs. 1 S. 2 LVwG-E legt aufgrund der Eingriffsintensität der nachträglichen Echtzeitidentifizierung (s.o. I. Allgemeine verfassungsrechtliche und unionsrechtliche Rahmenbedingungen eine entsprechend qualifizierte

Überprüfung nahe. Dies wird durch Art. 14 Abs. 5 S. 1 KI-VO verdeutlicht, nach welchem der Betreiber von Hochrisiko-KI-Systemen keine weiteren Maßnahmen allein aufgrund der Ausgabe des Systems erlassen darf, solange keine entsprechend qualifizierte Person das Ergebnis überprüft und bestätigt hat. Dies ist also für § 195c Abs. 1 S. 2 LVwG-E anzupassen.

VII. § 184 LVwG-E

1. Ausweitung der Datenerhebung an allgemein zugänglichen Orten

Die Anforderungen an die allgemeine Datenerhebung durch Video- und Tonaufnahmen aus den bisherigen § 184 Abs. 2 und 3 LVwG wurden neu gefasst und in § 184 Abs. 3 LVwG-E vereinheitlicht. Offene Bild- und Tonaufnahmen auf allgemein zugänglichen Flächen sollen nunmehr zulässig sein, wenn dies (1.) zur Abwehr einer Gefahr erforderlich ist oder es sich (2. und 3.) um besonders gefährdete Orte handelt.

Eine Erweiterung gegenüber der bisherigen Rechtslage besteht insbesondere darin, dass eine allgemeine Ermächtigung für das Anfertigen von Ton- und Videoaufnahmen zur Abwehr einer konkreten Gefahr für die öffentliche Sicherheit eingefügt worden ist (§ 184 Abs. 3 S. 1 Nr. 1 LVwG-E, vgl. Drs. 20/4284, S. 40). Die Überwachung von besonders gefährdeten Orten (§ 184 Abs. 3 Nr. 2 LVwG-E) wird darüber hinaus durch § 184 Abs. 3 Nr. 3 LVwG-E um die Überwachung von Orten i.S.d. § 181 Abs. 1 Nr. 1 bis 3 LVwG erweitert, wodurch etwa auch Verkehrs- und Versorgungsanlagen, öffentliche Verkehrsmittel und besonders geschützte Objekte überwacht werden können. Insgesamt erweitert sich damit also der Anwendungsbereich der Bild- und Tonüberwachung.

Die Daten aus dieser Überwachung werden die Grundlage der automatisierten und KI-gestützten Echtzeit-Fernidentifizierung nach § 184b LVwG-E. Wenn sich schon die erhobene Datengrundlage ausweitet, intensiviert sich in der Folge auch die Treffsicherheit und praktische Wirksamkeit der Fernidentifizierung. Die Erweiterung des Kreises überwachbarer Orte vergrößert zugleich den Kreis derjenigen, deren biometrische Merkmale bei einem Suchverlauf erfasst werden. Es tritt also eine Hebelwirkung ein. Diese wechselseitige Verstärkung sollte der Gesetzgeber bei der Bewertung der Grundrechtsrelevanz beachten.

2. Automatisierte Erkennung von Bewegungsmustern

Die Zulässigkeit von automatisierten Systemen in § 184 Abs. 5 LVwG-E ermöglicht das Erkennen von Bewegungsmustern. Dadurch wird neues, zuvor nicht verfügbares Wissen gewonnen. Dies führt zu einem eigenständigen Eingriffsgewicht, wie es das BVerfG für die automatisierte Datenauswertung anerkannt hat (BVerfGE 165, 363 (396 ff.) Rn. 69 f.). Ferner ist § 184

Abs. 5 S. 4 LVwG-E klarstellungsbedürftig. Nach dem Wortlaut der Vorschrift sind zwar „vorrangig nicht körperliche Merkmale zu verwenden“. Dennoch bleibt der Rückgriff auf körperliche Merkmale möglich. Werden diese zur Analyse von Gangbild oder vergleichbaren verhaltenstypischen Merkmalen genutzt, handelt es sich um biometrische Daten i.S.d. Art. 3 Nr. 34 KI-VO. Dadurch liegt es nahe, den Vorgang als biometrische Fernidentifizierung i.S.d. Art. 3 Nr. 41 KI-VO einzuordnen (vgl. Coombe/Roth-Isigkeit, ZfDR 2024, 391 (396)). Dem wird auch nicht durch den Ausschluss nach § 184 Abs. 5 S. 4 Hs. 2 LVwG-E begegnet, da dieser nur die „Identifizierung“ verbietet. Eine Wiedererkennung bleibt dabei möglich. Um dieser Möglichkeit entgegenzuwirken, sollte der Wortlaut der Regelung umformuliert werden. Denkbar wäre etwa folgender Wortlaut: „Zur Kennzeichnung nach Satz 3 dürfen nur nicht körperliche Merkmale verwendet werden; eine Verarbeitung biometrischer Daten ist nach dieser Vorschrift nicht zulässig.“

Anzumerken ist ferner, dass für die Maßnahme nach § 184 Abs. 5 LVwG-E kein vorheriger Richtervorbehalt vorgesehen ist und nur eine eingeschränkte Benachrichtigungspflicht bestehen soll, die nur bei Betrieb eines Hochrisiko-KI-Systems gemäß Art. 26 Abs. 11 KI-VO einschlägig ist. Die allgemeine Hinweispflicht gemäß § 184 Abs. 7 S. 3 LVwG-E genügt der ausdrücklichen Benachrichtigung über die Maßnahme für etwaige Rechtsschutzmöglichkeiten nicht. Auch angesichts der Anknüpfung an § 184 Abs. 3 S. 1 Nr. 1 LVwG-E, in welchem lediglich eine einfache Gefahr für die öffentliche Sicherheit für die offene Bild- und Tonaufnahme oder – aufzeichnung vorausgesetzt wird, besteht ein Wertungsgefälle gegenüber § 184b LVwG-E. Dieser beschränkt einerseits den Anwendungsbereich auf Leben, Leib, Freiheit und die sexuelle Selbstbestimmung und verlangt andererseits auch besonders hohe Eingriffshürden nach Art. 5 KI-VO.

Zwischen den Maßnahmen besteht insoweit ein Wertungsgefälle, das der Gesetzgeber schließen sollte.

VIII. Verfahren und technische Umsetzung

§ 184c Abs. 3 S. 3 LVwG-E verweist auf die Mitteilungspflichten nach Art. 5 Abs. 4 der KI-Verordnung. Sie sollen demnach dem Landespolizeiamt obliegen. Die Mitteilungspflicht erfordert, dass jede Verwendung eines biometrischen Echtzeit-Fernidentifizierungssystems in öffentlichen Räumen einerseits der zuständigen Marktüberwachungsbehörde und andererseits der nationalen Datenschutzbehörde mitgeteilt wird. Die zuständige Marktüberwachungsbehörde wird dabei durch § 2 Abs. 1 KI-MIG festgelegt. Es handelt sich um die Bundesnetzagentur. Diese Bestimmung gilt allerdings nur für eine Verwendung von KI-Systemen durch Bundesbehörden. Wenn dagegen Landesbehörden handeln, haben die Länder gemäß § 2 Abs. 6 KI-MIG

auch die zuständige Marktüberwachungsbehörde festzulegen. Soweit ersichtlich, ist die zuständige Marktüberwachungsbehörde vom Land Schleswig-Holstein bisher nicht benannt worden. Damit geht die Mitteilungspflicht ins Leere. Vor Inkrafttreten des Gesetzes muss also zwingend die zuständige Marktüberwachungsbehörde im Land Schleswig-Holstein benannt werden.

Für die Umsetzung der technisch-organisatorischen Einzelheiten sieht § 184c Abs. 3 S. 4 LVwG-E vor, dass das Innenministerium zum Erlass einer vereinheitlichenden Verwaltungsvorschrift ermächtigt wird. Sinnvoller wäre es, wenn das Innenministerium nicht nur ermächtigt, sondern verpflichtet wird, diese vereinheitlichende Verwaltungsvorschrift zu erlassen.

§ 195c Abs. 3 S. 4 LVwG-E trifft eine vergleichbare Bestimmung für die nachträgliche biometrische Fernidentifizierung. Auch hier sollte überdacht werden, ob eine Verpflichtung zum Erlass der Verwaltungsvorschrift nicht zweckmäßiger wäre.

IX. Schlussbemerkung

Insgesamt beinhaltet der Gesetzentwurf tiefgreifende Grundrechtseingriffe, an die das BVerfG hohe Hürden stellt. Auch das Unionsrecht beschränkt die Anwendung von KI-gestützter biometrischer Fernidentifizierung, wobei unterschiedlich hohe Ansprüche an die Echtzeit- und nachträgliche Fernidentifizierung gestellt werden.

Der Gesetzentwurf bildet diese Anforderungen ab. Unsicherheiten bestehen allerdings dahingehend, ob eine „konkrete Gefahr“ als Eingriffsschwelle ausreichend ist. Angesichts der besonderen Eingriffsintensität einer KI-gestützten Massenüberwachung wäre auch denkbar, dass das BVerfG eine höhere Eingriffsschwelle verlangt.

Die teils sehr technische und verschachtelte Formulierung der §§ 184b, 195b LVwG-E mit ihren vielen Verweisen auch auf unionsrechtliche Vorschriften dürfte die Rechtsanwendung erheblich erschweren. Das ist allerdings den zweigleisigen Anforderungen aus Verfassungs- und Unionsrecht geschuldet.

Abschließend sei darauf hingewiesen, dass die vorgeschlagenen Ausweitungen der polizeilichen Handlungsbefugnisse zum Teil ganz erhebliche Eingriffe in sensible Grundrechtsgüter erlauben. In diesen Eingriffen realisieren sich grundrechtliche Schutzpflichten zugunsten anderer, ebenfalls sehr oft gewichtiger Grundrechte. Dennoch muss der Gesetzgeber sich bei jeder dieser und auch bei künftigen Änderungen, in denen vor allem technische Entwicklungen aufgegriffen werden dürften, im Klaren sein, dass er den gefühlten und den tatsächlichen Freiheitsraum des Bürgers verengt. Der Staat hat sich für Eingriffe zu rechtfertigen; nicht der Bürger für die Freiheitsausübung. Dieses Vorrangprinzip darf nicht durch eine inkrementelle, je für sich genommen kleinschrittig wirkende Ausweitung behördlicher Befugnisse ausgehöhlt werden.

Außerdem muss der Gesetzgeber die Anwendung von diskriminierenden Algorithmen im Lichte von Art. 3 Abs. 1, 3 GG verhindern. Hierzu können Beobachtungs- und Nachsteuerungspflichten effektive Maßnahmen sein.

Neben den inhaltlichen Anmerkungen in Bezug auf die vorgeschlagenen Normen ist darauf hinzuweisen, dass der schleswig-holsteinische Gesetzgeber, sollten die Vorschriften beschlossen werden, diese binnen 30 Tagen der Kommission mitteilen muss (Art. 5 Abs. 5 S. 4 KI-VO).

X. Zusammenfassung der Ergebnisse

1. Das Bundesverfassungsgericht hat bisher nicht grundlegend über die Voraussetzungen der biometrischen Fernidentifizierung entschieden. Entsprechende Grundrechtseingriffe dürften aber bei einer konkreten Gefahr für besonders wichtige Rechtsgüter (Leib, Leben, Freiheit, sexuelle Selbstbestimmung einer Person, Bestand des Bundes oder eines Landes) gerechtfertigt sein. Es ist aber angesichts der besonderen Sensibilität der relevanten Freiheitsrechte und angesichts der zur Diskussion stehenden Eingriffsintensität nicht ausgeschlossen, dass das Bundesverfassungsgericht noch höhere Maßstäbe für eine KI-gestützte Identifizierung aufstellt.
2. Die Betroffenheit von unbeteiligten Dritten tritt durch die massenweise Verarbeitung ihrer biometrischen Daten und durch „chilling effects“ ein, die deren Grundrechtsausübung behindern könnten. Dieser Umstand spricht dafür, dass der Gesetzgeber hier besonders hohe verfassungsrechtliche Hürden zu beachten hat.
3. §§ 184b, 195b LVwG-E erfüllen die verfassungsrechtlichen Mindestvoraussetzungen.
 - a. Die Eingriffsschwellen könnten aber zur Sicherheit auf eine „dringende Gefahr“ erhöht werden. Diese Eingriffshürde dürfte auch dann einer verfassungsgerichtlichen Prüfung standhalten, wenn das Bundesverfassungsgericht eine ganz besonders hohe Eingriffsintensität annimmt.
 - b. Die Verwendung des Begriffs der „unbedingten Erforderlichkeit“ ist unionsrechtlich geboten und gewährleistet die verhältnismäßige Anwendung der Normen.
4. Der Gesetzentwurf enthält ausreichende rechtsstaatliche Hürden. Vor diesem Hintergrund überzeugen auch die Berichts- und Protokollpflichten nach §§ 184c Abs. 3, 186b, 186c LVwG-E.

5. Es ist streng zwischen der Echtzeit-Fernidentifizierung und der nachträglichen Fernidentifizierung zu differenzieren. Die besonderen unionsrechtlichen Hürden beziehen sich in erster Linie auf die Echtzeit-Fernidentifizierung. Verfassungsrechtlich sind die Anforderungen hingegen weitgehend gleich. Dem trägt der Gesetzentwurf ausreichend Rechnung.
6. Die Herkunft von Referenzdaten für Fernidentifizierungen ist verfassungsrechtlich erheblich. Die Eingriffsintensität steigt, wenn offene und massenhafte Datenräume durchsucht werden. Die §§ 195b, 195c LVwG-E entsprechen den Anforderungen des BVerfG an eine qualifizierte Ermächtigungsgrundlage.
7. Das Absehen von einem zeitlichen Höchstmaß und die Befristung der Maßnahme auf sieben Tage überzeugen in der Kombination, da auf diese Weise eine effektive Gefahrenabwehr ermöglicht wird.
8. Die Formulierung „zwei qualifizierte Beschäftigte der Polizei“ ist hinsichtlich des Merkmals der Qualifikation zu unspezifisch.
9. Wenn mit § 184 LVwG-E die Grundlage der Datenerhebung ausgeweitet wird, steigt auch die Eingriffsintensität der KI-gestützten Echtzeit-Fernidentifizierung (§ 184b LVwG-E) spiegelbildlich an. Der Gesetzgeber muss die Wechselwirkungen zwischen diesen Normen bei der Ausgestaltung berücksichtigen.
10. §§ 184c Abs. 3 S. 4, 195c Abs. 3 S. 4 LVwG-E sollten dahingehend angepasst werden, dass der Erlass einer Verwaltungsvorschrift zur Regelung technisch-organisatorischer Einzelheiten nicht nur möglich, sondern verpflichtend ist.

Für Rückfragen stehe ich jederzeit zur Verfügung.

Mit freundlichen Grüßen

Professor Dr. Florian Becker