

Schleswig-Holsteinischer Landtag
Umdruck 20/6959

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

für den Innen- und Rechtsausschuss des Schleswig-Holsteinischen Landtages

14. August 2026

Univ.-Prof. Dr. Dirk Heckmann

Inhaber des Lehrstuhls für Recht und Sicherheit der Digitalisierung

Ass. iur. Joanna Klauser

Wiss. Referentin am Bayerischen Forschungsinstitut für Digitale Transformation

Ass. iur. Nicolas Ziegler

Geschäftsführer des TUM Center for Digital Public Services

I.	Vorbemerkung.....	4
1.	Gegenstand dieses Gutachtens	4
2.	Anwendbare Grundrechtsordnung.....	4
II.	IT-gestützter Abgleich und Datenanalyse (§§ 188c, 188d LVwG-E).....	5
1.	Unionsrechtliche Bewertung.....	5
a)	Datenschutzrecht.....	5
b)	KI-VO	5
2.	Verfassungsrechtliche Bewertung	6
a)	Maßstäbe zur Bestimmung des Eingriffsgewichts polizeilicher Datenanalysen 7	
b)	Eingriffsgewicht des IT-gestützten Abgleichs und der Datenanalyse	9
aa)	IT-gestützter Abgleich	9
bb)	Datenanalyse.....	9
c)	Rechtfertigungsanforderungen des IT-gestützten Abgleichs und der Datenanalyse	11
aa)	IT-gestützter Abgleich	11
bb)	Datenanalyse.....	11
III.	Biometrische Fernidentifizierung	12
IV.	Echtzeit-Fernidentifizierung in öffentlich zugänglichen Räumen, §§ 184b, 184c LVwG-E	13
1.	Erfordernis einer gesetzlichen Grundlage.....	13
2.	Sekundärrechtliche Vorgaben des Europarechts	14
3.	Verfassungsrechtliche Voraussetzungen	14
4.	Einzelne Aspekte der Norm	16
a)	Gemeinsame Einsatzbedingungen von Systemen mit und ohne Qualifikation als KI-System i.S.d. KI-VO	16
b)	Vier-Augen-Prinzip und Qualifikation der Zugangsberechtigten.....	17
c)	Prinzip der Normenklarheit.....	18
V.	Nachträgliche Fernidentifizierung unter Einbeziehung von Bildern aus dem Internet gem. §§ 195b, 195c LVwG-E	18

1. Erfordernis einer gesetzlichen Grundlage.....	18
2. Verbot des Art. 5 Abs. 1 lit. e KI-VO	18
3. Gleichwertigkeit der Eingriffstiefe durch nachträgliche Fernidentifizierung gegenüber der Echtzeit-Fernidentifizierung.....	20
4. Verfassungsrechtliche Bedenken	20
5. Zwischenfazit.....	21
6. Einzelne Aspekte der Norm	21
a) Gemeinsame Einsatzbedingungen von Systemen mit und ohne Qualifikation als KI-System i.S.d. KI-VO	21
b) Vier-Augen-Prinzip und Qualifizierung der Zugangsberechtigten	22
VI. Abschließende Bemerkungen	22
1. Digitale Souveränität.....	22
2. Totalüberwachungsverbot	22
3. Transparenz und Rechtsschutz	23
4. Evaluation	24
5. Fazit und abschließende Handlungsempfehlungen	24

I. Vorbemerkung

1. Gegenstand dieses Gutachtens

Der Entwurf eines Gesetzes zur Fortentwicklung polizeirechtlicher Maßnahmen für einen wirksamen Schutz der öffentlichen Sicherheit wird mit der Notwendigkeit begründet, auf die Zunahme von „Messerangriffen“ im öffentlichen Raum durch neue bzw. erweiterte Polizeibefugnisse reagieren zu müssen. Rechtspolitisch kann diese Notwendigkeit unterschiedlich beurteilt werden.

Die vorliegende gutachterliche Stellungnahme beschränkt sich demgegenüber auf die rechtsdogmatische, insbesondere verfassungsrechtliche Perspektive und zielt darauf, dem Gesetzgeber Hinweise zur verfassungs- und europarechtskonformen Ausgestaltung der Befugnisnormen zu geben. Die Autoren konzentrieren sich dabei auf die Begutachtung der Vorschriften, die in ihrem Forschungsfokus liegen und besonderen Anlass geben: der IT-gestützte Datenabgleich und die Datenanalyse (§§ 188c, 188d LVwG-E), die Echtzeit-Fernidentifizierung in öffentlich zugänglichen Räumen (§§ 184b, 184c LVwG-E) sowie die nachträgliche Fernidentifizierung unter Einbeziehung von Bildern aus dem Internet (§§ 195b, 195c LVwG-E).

2. Anwendbare Grundrechtsordnung

Die gutachterliche Stellungnahme stützt sich hinsichtlich der Bewertung der Verfassungskonformität der betrachteten Normen auf die Grundrechte des GG. Durch die zunehmende Europäisierung der Sicherheitsgewährleistung und insb. die sicherheitsrechtlichen Regelungsgehalte der KI-VO ist die im Zusammenhang sicherheitsbehördlichen Einsatzes künstlicher Intelligenz anwendbare Grundrechtsordnung nicht mehr von vornherein eindeutig.¹ Angesichts der noch gänzlich offenen Rechtsfragen zur Auslegung von Art. 51 Abs. 1 S. 1 GRCh und des ungeklärten Harmonisierungsgrads der KI-VO ist es weder Anliegen noch Aufgabe dieses Gutachtens, Klarheit über die anwendbare Grundrechtsordnung zu schaffen.²

Die Stellungnahme arbeitet daher hinsichtlich der angewandten Grundrechtsordnung mit folgenden Annahmen: Zur Abgrenzung zwischen GG und GRCh werden die Grundsätze herangezogen, welche das BVerfG entwickelt hat.³ Danach finden nur im unionsrechtlich vollständig determinierten Bereich ausschließlich die Unionsgrundrechte Anwendung.⁴ Noch ungeklärt ist, ob es sich bei den Vorschriften der KI-VO zu verbotenen Praktiken um

¹ Umfassend hierzu Hofmann-Coombe, EuR 2025, 363 ff. Schon die bisherige Rechtslage hinsichtlich der Anwendbarkeit der konkreten Grundrechtsordnung im Bereich der sicherheitsbehördlichen Datenverarbeitung war aber längst nicht so eindeutig, wie die Literatur und Rspr. des BVerfG zum Sicherheitsverfassungsrecht des GG suggeriert haben.

² Vgl. zum bisherigen Verhältnis von GRCh zum GG im Sicherheitsrecht Müller/Schwabenbauer, in: Lisken/Denninger PolR-HdB, 7. Aufl. 2021, G. Rn. 385 ff.

³ Hofmann-Coombe, EuR 2025, 363 (375) m.w.N.

⁴ BVerfGE 152, 216 (233 Rn. 42 ff.).

vollharmonisiertes Recht handelt.⁵ Dann wären die Maßnahmen nach der Rechtsprechung des BVerfG nicht an den Grundrechten des GG, sondern an der GRCh zu messen.⁶

Angesichts der diesbezüglich bestehenden Unsicherheiten, der ausdifferenzierteren Rechtsprechung des BVerfG und dem hieraus folgenden hohen Schutzstandard sowie der im Detail noch klärungsbedürftigen Kompetenz der europäischen Union im Sicherheitsrecht, wird der Fokus im Folgenden auf die Grundrechte des GG gelegt.

II. IT-gestützter Abgleich und Datenanalyse (§§ 188c, 188d LVwG-E)

Der Entwurf schafft neben bestehenden Formen des Datenabgleichs⁷ zwei neue Formen, den IT-gestützten Abgleich i.S.v. § 188c Abs. 1 LVwG-E und die Datenanalyse i.S.v. § 188c Abs. 2 LVwG-E. Der Entwurf will die Sicherheitsgewährleistung durch die Nutzung von Künstlicher Intelligenz und automatisierter Datenanalyse verbessern.⁸ Die neuen Befugnisse sollen insbesondere die „Weiternutzung großer und komplexer Informationsbestände“⁹ ermöglichen und sowohl Grenzen der technischen Interoperabilität als auch der bisherigen kriminalistischen Erkenntnisfähigkeit ausdehnen.¹⁰

Die beiden vorgeschlagenen Formen des Datenabgleichs in §§ 188c, 188d LVwG-E werden nachfolgend auf ihre Vereinbarkeit mit höherrangigem Recht untersucht. Soweit sinnvoll, werden darüber hinaus auch Hinweise zur Gesetzessystematik und zur künftigen Rechtsanwendung gegeben.

1. Unionsrechtliche Bewertung

a) Datenschutzrecht

Gem. § 43 LDSG (SH), welcher Art. 27 JI-RL (RL (EU) 2016/680) umsetzt, ist vor Inbetriebnahme einer Analysesoftware zwingend eine Datenschutz-Folgenabschätzung durchzuführen. Diese darf nicht abstrakt die Rechtsgrundlagen beleuchten, sondern muss auch und gerade die gewählte technische Umsetzung bewerten.

b) KI-VO

Auch wenn im Rahmen der Datenanalyse i.S.v. § 188c Abs. 3 LVwG-E der Einsatz selbstlernender Künstlicher Intelligenz verboten bleibt (§ 188c Abs. 6 S. 2 Nr. 2 LVwG-E) sind die Anforderungen der KI-VO von Relevanz. Trotz Wortlaut und ErwGr der KI-VO fallen nach einer teleologisch-extensiven Auslegung der Begriffsbestimmung des KI-Systems

⁵ Für Art. 5 KI-VO und insbesondere die biometrische Fernidentifizierung von vollharmonisiertem Recht ausgehend, Hofmann-Coombe, EuR 2025, 363 (378); Für nachträgliche Fernidentifizierung Hofmann-Coombe, EuR 2025, 363 (380); a.A. Hahn, Automatisierte Gesichtserkennung in der Strafverfolgung, 2025, S. 203f.

⁶ BVerfGE 152, 216 (233) Rn. 42f.

⁷ §§ 195, 195a LVwG.

⁸ LT-Drs. 20/4284, S. 3.

⁹ LT-Drs. 20/4284, S. 3.

¹⁰ LT-Drs. 20/4284, S. 30 f.

i.S.v. Art. 3 Nr. 1 KI-VO auch deterministische, nicht selbstlernende Systeme unter diesen Begriff.¹¹

Nach Art. 5 Abs. 1 lit. d Hs. 1 KI-VO ist Predictive Policing, welches sich auf konkrete Personen und nicht etwa gefährliche Orte bezieht, generell verboten. § 188c Abs. 7 S. 3 LVwG-E will ein Predictive Policing ausschließen.¹² Die im Referentenentwurf noch enthaltene Einschränkung dieses Verbots, das anlassbezogenes Predictive Policing zugelassen hätte, wurde begrüßenswerterweise entfernt. Nach Art. 5 Abs. 1 lit. d Hs. 2 KI-VO ist Predictive Policing nur soweit zulässig, wie menschlich vorgenommene Bewertungen unterstützt werden.¹³

Da §§ 188c, 188d LVwG-E das Erstellen von Profilen i.S.v. Art. 3 Abs. 4 JI-RL im Grundsatz erlauben, handelt es sich insoweit um Hochrisiko-KI i.S.v. Art. 6 Abs. 2 i.V.m Anhang III Nr. 1 lit. d KI-VO. Für diesen konkreten Anwendungsbereich sind daher die Pflichten der Art. 6 ff. KI-VO einzuhalten. Angesichts der hohen Transparenzvorgaben und technischen wie organisatorischen Anforderungen der §§ 188c und 188d LVwG-E liegt ein Verstoß gegen Kapitel III Abschnitt 2 der KI-VO nicht nahe. Der Entwurf verweist in § 188d Abs. 4 S. 3 und Abs. 6 S. 3 LVwG-E auf die Betreiberpflichten der KI-VO hin. Ein Verstoß gegen das europarechtliche Normwiederholungsverbot kann darin nicht gesehen werden.

2. Verfassungsrechtliche Bewertung

Maßgeblicher Prüfstein der Vorschriften zur Datenanalyse ist die Entscheidung des BVerfG zur Datenanalyse nach § 25a HSOG und § 49 HmbPolDVG.¹⁴ Hier hat das BVerfG grundsätzliche Maßstäbe für die verfassungsrechtliche Bewertung dieser Befugnis-kategorie aufgestellt.

Nach diesen Grundsätzen stellt die Auswertung bestehender personenbezogener polizeilicher Daten, also sowohl der IT-gestützte Abgleich nach § 188c Abs. 1 LVwG-E als auch die Datenanalyse nach § 188c Abs. 2 LVwG-E, einen Eingriff in das Recht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG dar, weil diese Nutzung den ursprünglichen Erhebungszweck verläßt und daher nach den Grundsätzen der Zweckbindung einen eigenständigen und neuen Eingriff darstellt.¹⁵ Im Fall der hier einzuführenden Datenanalyse ergibt sich ein Eingriff aber nicht nur durch die zusammenführende Verwendung der Daten, sondern auch durch die analysegestützte Erlangung neuen Wissens.¹⁶

¹¹ Wendehorst, in: Martini/Wendehorst, 1. Aufl. 2024, KI-VO Art. 3 Rn. 32 ff.; speziell für das Sicherheitsrecht Benamor, BayVBl 2025, 44 (48 f.) und Hofmann-Coombe, EuR 2025, 363 (368 ff.).

¹² LT-Drs. 20/4284, S. 53.

¹³ Vgl. Wendehorst, in: Martini/Wendehorst, 1. Aufl. 2024, KI-VO Art. 5 Rn. 85.

¹⁴ BVerfGE 165, 363 – *Automatisierte Datenanalyse*.

¹⁵ BVerfGE 165, 363 (388 Rn. 50, 390 ff. Rn. 55 ff.); 141, 220 (324 Rn. 277, 327 Rn. 285).

¹⁶ BVerfGE 165, 363 (388 f. Rn. 50, 395 ff. Rn. 67 ff.).

Die konkreten verfassungsrechtlichen Anforderungen – welche das BVerfG v.a. aus der Verhältnismäßigkeit im engeren Sinne schöpft – bemessen sich anhand zahlreicher im Urteil entwickelter abstrakter Maßstäbe, welche das spezifische Eingriffsgewicht einer Datenanalyse bestimmen. Im Folgenden werden diese Maßstäbe kurz referiert (a.), ehe für den IT-gestützten Abgleich i.S.v. 188c Abs. 1 LVwG-E und die verschiedenen Varianten der Datenanalyse i.S.v. § 188c Abs. 2 LVwG-E das konkrete Eingriffsgewicht bestimmt wird (b.), um daraus letztlich die Rechtfertigungsanforderungen zu gewinnen und die Rechtsgrundlagen danach zu bewerten (c.).

a) **Maßstäbe zur Bestimmung des Eingriffsgewichts polizeilicher Datenanalysen**

Die Bewertung der Eingriffsintensität einer Datenanalyse erfolgt in zwei Stufen: Erstens ist die Intensität der ursprünglichen Informationseingriffe zur Erhebung der Daten zu bestimmen, ehe zweitens das Eigengewicht der automatisierten Datenanalyse addiert wird.¹⁷ Angesichts des Umfangs und Anlasses dieser Stellungnahme konzentriert sich die nachfolgende Darstellung auf das Eigengewicht des Grundrechtseingriffs, den die Datenanalyse bewirkt.

Die Eingriffstiefe wird beeinflusst durch folgende Parameter:

- **Persönlichkeitsrelevanz** bzw. Sensibilität der zusammengeführten und analysierten Daten.¹⁸
- Risiko **Unbeteiligter**, das „Ziel weiterer polizeilicher Aufklärungsmaßnahmen zu werden“.¹⁹
- Risiko der **Diskriminierung** anhand unzulässiger Kriterien i.S.v. Art. 3 Abs. 3 GG.²⁰
- **Umfang** bzw. Menge der zusammengeführten und analysierten Daten.²¹
- Insb. eingriffsverstärkend wirkt der Einbezug des **Internets** in die Auswertung.²²
- **Komplexität** der eingesetzten Analysesoftware bzw. zugelassene Analysemethodik:²³ „Insgesamt ist die Methode automatisierter Datenanalyse oder -auswertung umso eingriffsintensiver, je breitere und tiefere Erkenntnisse über Personen dadurch erlangt werden können, je höher die Fehler- und Diskriminierungsanfälligkeit ist und je schwerer die softwaregestützten Verknüpfungen nachvollzogen

¹⁷ BVerfGE 165, 363 (390 Rn. 54).

¹⁸ BVerfGE 165, 363 (400 f. Rn. 77). Das Eingriffsgewicht erhöht sich, je privater die Informationen sind und wenn „ein Bewegungs- oder Verhaltensprofil einer Person oder ein umfassenderes Persönlichkeitsbild entstehen kann.“

¹⁹ BVerfGE 165, 363 (400 f. Rn. 77) m.w.N.

²⁰ BVerfGE 165, 363 (400 f. Rn. 77).

²¹ BVerfGE 165, 363 (401 Rn. 78): „Je größere Mengen personenbezogener Daten in die automatisierte Datenanalyse und -auswertung einbezogen werden können, je weniger der Gesetzgeber also die verwendbare Datenmenge begrenzt, umso schwerer wiegt der Eingriff.“

²² BVerfGE 165, 363 (404 Rn. 88).

²³ BVerfGE 165, 363 (404 f. Rn. 90 f.).

werden können.“²⁴ Besonders eingriffsintensiv ist daher der Einsatz **selbstlernender** Systeme,²⁵ wobei die eingriffsintensivierenden Folgen bereits bei **deterministischen** Systemen eintreten können.²⁶

- **Fehleranfälligkeit** der Software.²⁷
- Ausgabe maschineller Bewertungen i.S.e. **Predictive Policing**.²⁸
- Unbeschränktheit möglicher **Suchergebnisse**.²⁹
- **Rechtsschutzdefizite** und Heimlichkeit der Maßnahme.³⁰

Folgende Umstände vermögen es, das Eingriffsgewicht zu mitigieren:

- Beschränkung der Herkunft von Daten.³¹
- Ausschluss von Daten aus **schwerwiegenden Informationseingriffen**.³²
- Beschränkung auf Daten von Personen, die einen **zurechenbaren Anlass** zur Verarbeitung ihrer Daten gegeben haben.³³
- **Reduzierung der Datenmenge** durch Aufbewahrungsfristen, Löschpflichten und zügigem Löschen von Nichttreffern.³⁴
- Ausschluss der Verarbeitung **biometrischer Daten**.³⁵
- Händischer statt automatischer Einbezug breitenwirksamer oder sensibler Datenquellen.³⁶
- **Zugangsbeschränkungen** und Durchführung der Analysen durch bes. qualifiziertes Personal.³⁷
- Weitere Voraussetzungen zur Verwendung der durch die Analyse erzielten Ergebnisse.³⁸
- Vorkehrungen zur **Korrektur von Fehlern** der Software.³⁹

²⁴ BVerfGE 165, 363 (404 f. Rn. 90).

²⁵ BVerfGE 165, 363 (408 Rn. 100).

²⁶ BVerfGE 165, 363 (409 Rn. 101).

²⁷ BVerfGE 165, 363 (409 Rn. 102).

²⁸ BVerfGE 165, 363 (407 Rn. 98).

²⁹ BVerfGE 165, 363 (407 Rn. 97).

³⁰ BVerfGE 165, 363 (399 f. Rn. 76).

³¹ BVerfGE 165, 363 (401 Rn. 79).

³² BVerfGE 165, 363 (402 Rn. 81).

³³ BVerfGE 165, 363 (403 Rn. 84).

³⁴ BVerfGE 165, 363 (403 f. Rn. 85 f.).

³⁵ BVerfGE 165, 363 (404 Rn. 87).

³⁶ BVerfGE 165, 363 (404 Rn. 88).

³⁷ BVerfGE 165, 363 (404 Rn. 89).

³⁸ BVerfGE 165, 363 (407 f. Rn. 99).

³⁹ BVerfGE 165, 363 (409 Rn. 102).

b) Eingriffsgewicht des IT-gestützten Abgleichs und der Datenanalyse

Legt man die eben gefundenen Maßstäbe zusammen, ergibt sich folgendes Bild:

aa) IT-gestützter Abgleich

Der IT-gestützte Abgleich nach § 188c Abs. 1 LVwG-E ist als niedrigschwelliger Abgleich konzipiert.⁴⁰ Erlaubt werden lediglich gezielte Abfragen in die begrenzten Quellen i.S.v. § 188c Abs. 3 S. 1 LVwG-E. Im Ergebnis handelt es sich um einen einfachen Datenabgleich, dessen **Eingriffsgewicht** als **gering** zu bewerten ist.⁴¹

bb) Datenanalyse

Die Datenanalyse nach § 188c Abs. 2 LVwG-E weist in den nachfolgenden Absätzen und in § 188d LVwG-E, wo Voraussetzungen und begleitende Verfahrensvorschriften geregelt sind, unterschiedliche Eingriffsschwellen auf: § 188c Abs. 3 LVwG-E soll die Datenanalyse mit „reduziertem“ Eingriffsgewicht regeln,⁴² § 188c Abs. 4 LVwG-E regelt die Datenanalyse mit hohem Eingriffsgewicht.⁴³ Die Differenzierung des Eingriffsgewichts ergibt sich durch die differenzierte Anwendung der eingriffssteuernden Parameter in § 188c Abs. 5 ff. LVwG-E und § 188d LVwG-E. Die nachfolgende Darstellung erfolgt daher getrennt.

Datenanalyse mit reduziertem Eingriffsgewicht i.S.v. § 188c Abs. 3 LVwG-E

Der Verweis von § 188c Abs. 2 LVwG-E auf § 188a Abs. 1 und 2 LVwG sowie § 479 Abs. 2 S. 2 Nr. 1 StPO sichert die Einhaltung der Grundsätze der Zweckbindung und stellt klar, dass eine Datenanalyse immer nur zweckgebunden erfolgen kann.⁴⁴ Eingriffsmildernd wirkt die Beschränkung in § 188c Abs. 3 LVwG-E auf einige ausgewählte polizeiliche Informationsquellen. § 188c Abs. 5 LVwG-E reduziert das Eingriffsgewicht zusätzlich durch die Beschränkung, dass Informationen aus Registern und dem Internet nur händisch und im Einzelfall einbezogen werden dürfen. § 188c Abs. 6 LVwG-E reduziert das Eingriffsgewicht merklich. Sowohl die Sensibilität und die Menge der auszuwertenden Daten als auch die Auswertungsmethode werden eingeschränkt. § 188c Abs. 6 S. 2 Nr. 2 LVwG-E beschränkt die anwendbare Software auf deterministische Systeme. Positiv hervorzuheben ist der Ausschluss von Daten nach § 188c Abs. 6 S. 1 LVwG-E, die durch besonders eingriffsintensive heimliche Überwachungsmaßnahmen erhoben wurden. § 188c Abs. 7 LVwG-E schließt die Bildung von Verhaltens- und Bewegungsprofilen für die Datenanalyse mit eingriffsreduziertem Eingriffsgewicht nicht aus, sondern beschränkt sie nur auf den Zeitraum einer Woche. Diese Einschränkung ist angesichts der Tatsache, dass sich

⁴⁰ LT-Drs. 20/4284, S. 50.

⁴¹ Vgl. BVerfGE 165, 363 (398 f. Rn. 72, 74; 405 Rn. 91).

⁴² LT-Drs. 20/4284, S. 51

⁴³ LT-Drs. 20/4284, S. 52.

⁴⁴ § 188c Abs. 2 S. 1 und S. 2 LVwG-E. Eine vollständig anlasslose Datenanalyse wäre mit der Verfassung unvereinbar und nicht zu rechtfertigen.

schon mit bloßen Verkehrsdaten in einer Woche umfassende Profile erstellen lassen,⁴⁵ zur Eingriffsreduktion nicht geeignet. Personenbezogenes Predictive Policing wird durch § 188c Abs. 7 S. 3 LVwG-E untersagt. § 188c Abs. 8 Nr. 1 LVwG-E i.V.m. § 186 Abs. 2 LVwG zwingt zur ausdrücklichen Anordnung mit Behördenleiterprivileg. Eine Profilbildung ist schriftlich anzuordnen. In § 188d LVwG-E finden sich noch zahlreiche eingriffsmildernde Verfahrensvorschriften, wie etwa

- die Einschränkung der Suche auf anlassbezogene Kriterien, wodurch offene Suchen ausgeschlossen werden (Abs. 2);
- Nachvollziehbarkeit der eingesetzten Software und eine antidiskriminierungsorientierte Auswahl der Suchkriterien (Abs. 3);
- Begrenzung des Zugriffs auf die Anwendung (Abs. 4);
- Löschung der zusammengeführten Datensammlung (Abs. 5) und
- eine den Rechtsschutz ermöglichende Benachrichtigung Betroffener (Abs. 6).

Hinsichtlich des Eingriffsgewichts der Datenanalyse i.S.v. § 188c Abs. 3 LVwG-E ist der Entwurf sichtlich darum bemüht, die durch das BVerfG vorgezeichneten Möglichkeiten zu nutzen, die zu einer Eingriffsreduktion führen. Großteils ist das gelungen. Im Falle der Bildung von Bewegungs- oder Verhaltensprofilen ergibt sich jedoch weiterhin ein massives Eingriffsgewicht.⁴⁶ Lässt man die Profilbildung außen vor, ergibt sich eine **mittlere Eingriffsintensität**.⁴⁷

Datenanalyse mit hohem Eingriffsgewicht i.S.v. § 188c Abs. 4 LVwG-E

Die Datenanalyse nach § 188c Abs. 4 LVwG-E sieht ebenfalls zahlreiche Maßnahmen zur Mitigation des Eingriffsgewichts vor. § 188c Abs. 5 S. 1 LVwG-E verbietet die Anbindung ans Internet und polizeifremde Register dürfen nur händisch und im Einzelfall einbezogen werden. § 188c Abs. 6 S. 2 LVwG-E gilt auch für die eingriffshohe Variante der Datenanalyse, weshalb auch hier die Verarbeitung biometrischer Daten, ein Abgleich mit dem offenen Internet und der Einsatz selbstlernender Systeme untersagt bleibt. Erheblich eingriffsmildernd wirkt der Richtervorbehalt für die Anordnung einer eingriffsintensiven Datenanalyse nach § 188c Abs. 8 S. 2 Nr. 2 LVwG-E. Die Verfahrensvorschriften in § 188d LVwG-E gelten auch für die Datenanalyse nach § 188c Abs. 4 LVwG-E. Trotz ergriffener gesetzgeberischer Maßnahmen zur Minderung der **Eingriffsintensität** ist diese, wie

⁴⁵ Tokmetzis, Wie dein unschuldiges Smartphone fast dein ganzes Leben an den Geheimdienst übermittelt, netzpolitik.org vom 29.07.2014; vgl. auch die Studie von Perez/Musolesi/Stringhini, You are your Metadata: Identification and Obfuscation of Social Media Users using Metadata Information, 2018, <https://arxiv.org/abs/1803.10133>.

⁴⁶ Vgl. zur verfassungsrechtlichen Bewertung sicherbehördlicher Profilbildung Ziegler, RW 2024, 374 (380); Ziegler, in: Botta et al., Rechtsfragen virtueller Welten, 2025, S. 85 ff.

⁴⁷ Wie sie in BVerfGE 165, 363 (411 f. Rn. 107) beschrieben wird.

schon selbst erkannt,⁴⁸ **sehr hoch**. Dies ergibt sich insbesondere daraus, dass die Verarbeitung von Daten aus einer akustischen Wohnraumüberwachung (§ 188c Abs. 4 S. 2 LVwG-E), von Funkzellenabfragen (e.c. § 188c Abs. 5 S. 2 LVwG-E) und Eingriffen in informationstechnische Systeme (Quellen-TKÜ und Online-Durchsuchung; § 188c Abs. 6 S. 1 LVwG-E) zugelassen ist. Auch die zeitliche Begrenzungen der zur Bildung von Profilen nutzbaren Daten in § 188c Abs. 7 S. 2 LVwG-E gilt nicht für die Datenanalyse nach § 188c Abs. 4 LVwG-E.⁴⁹

c) Rechtfertigungsanforderungen des IT-gestützten Abgleichs und der Datenanalyse

Die anvisierte „Überwindung technischer Grenzen“⁵⁰ im Umgang mit polizeilich verfügbaren Daten durch die hier skizzierten Maßnahmen ist im Rahmen der Verhältnismäßigkeit ein legitimer Zweck, der geeignet und erforderlich ist.⁵¹ Von näherem Interesse sind hier nur die speziellen Anforderungen an die Rechtsgrundlagen der Datenanalyse, welche das BVerfG im Rahmen der Verhältnismäßigkeit im engeren Sinne formuliert hat. Wie streng die Anforderungen hier sind, bestimmt sich anhand der eben festgestellten Eingriffsintensität.⁵²

aa) IT-gestützter Abgleich

Für die Eingriffsschwelle des IT-gestützten Abgleichs nach § 188c Abs. 1 LVwG-E verweist die Norm auf § 188a Abs. 1, 2 LVwG und § 479 Abs. 2 S. 2 Nr. 1 und 2 StPO. Dort werden die Voraussetzungen und Grundlagen der Zweckänderung wiedergeben. Angesichts der geringen Eingriffsintensität des einfachen Abgleichs reichen die Grundsätze der Zweckbindung als Eingriffsschwelle aus.⁵³

bb) Datenanalyse

Beide Varianten der Datenanalysen des § 188c LVwG-E überwinden bisher bestehende Erkenntnisgrenzen, worin ihre spezifische Grundrechtssensibilität liegt.⁵⁴ Diesem höheren Eingriffsgewicht wird der Grundsatz der Zweckbindung nicht mehr gerecht.⁵⁵ Daher braucht es hier zusätzliche Anforderungen, um die Verhältnismäßigkeit im engeren Sinne zu wahren. Das BVerfG verlangt je nach individuellem Eingriffsgewicht unterschiedliche Eingriffsschwellen und unterschiedlich gewichtige Rechtsgüter, deren Schutz bezweckt ist.⁵⁶

⁴⁸ LT-Drs. 20/4284, S. 52.

⁴⁹ Zur sich daraus ergebenden Gefahr der Bildung eines verfassungsrechtlich unzulässigen umfassenden Persönlichkeitsbilds siehe später unter VI.2.

⁵⁰ LT-Drs. 20/4284, S. 30.

⁵¹ Vgl. BVerfGE 165, 363 (389 Rn. 52 f.).

⁵² BVerfGE 165, 363 (388 Rn. 49, 399 Rn. 75).

⁵³ Vgl. BVerfGE 165, 363 (412 Rn. 108).

⁵⁴ Vgl. BVerfGE 165, 363 (397 Rn. 70).

⁵⁵ BVerfGE 165, 363 (398 Rn. 72).

⁵⁶ BVerfGE 165, 363 (409 f. Rn. 103).

Für die **Datenanalyse in § 188c Abs. 3 LVwG-E** ergibt sich grds. ein mittleres bis gehobenes Eingriffsgewicht. Hierfür reicht es, Rechtsgüter von erheblichem Gewicht zu schützen.⁵⁷ Hinsichtlich der Eingriffsschwelle wäre es sogar möglich, weit in das Gefahrenvorfeld zu gehen.⁵⁸ Hiervon macht der Entwurf bewusst⁵⁹ keinen Gebrauch und formuliert in § 188c Abs. 3 S. 1 LVwG-E die drohende⁶⁰/konkretisierte Gefahr als Eingriffsschwelle. Im Grundsatz erfüllt die Maßnahme daher die Anforderungen des BVerfG. Das gilt jedoch nicht, soweit § 188c Abs. 3 i.V.m. Abs. 7 LVwG-E zur Anfertigung von Bewegungs- oder Verhaltensprofilen ermächtigt. Das BVerfG erachtet jegliche Profilbildung als schweren Eingriff in das Recht auf informationelle Selbstbestimmung,⁶¹ welche nur unter den hier nicht eingehaltenen Voraussetzungen für heimliche Überwachungsmaßnahmen angeordnet werden kann.

Für die **Datenanalyse nach § 188c Abs. 4 LVwG-E** ergibt sich ein hohes Eingriffsgewicht, weshalb diese nur unter den Voraussetzungen zulässig ist, die das BVerfG in der Vergangenheit für heimliche Überwachungsmaßnahmen angewendet hat.⁶² Diese Voraussetzungen sind hier gewahrt. Insbesondere das Rechtsgut der sexuellen Selbstbestimmung gehört auch zu den besonders gewichtigen Rechtsgütern.⁶³

III. Biometrische Fernidentifizierung

Mit dem Gesetz würde die biometrische Fernidentifizierung in verschiedenen Formen Einzug in das Sicherheitsrecht Schleswig-Holsteins finden.

Biometrische Fernidentifizierung nutzt biometrische Merkmale einer Person, um diese zu identifizieren. Beispielsweise wird bei Gesichtserkennungssoftware die Identifizierung eines Gesichts ermöglicht, indem das System ein sog. Template erstellt und mit anderen Templates abgleicht.⁶⁴ Für die Erstellung eines Templates werden die spezifischen Merkmale des Gesichts durch Analyse von Bildmaterial und/oder Videoaufnahmen einer Person erfasst.⁶⁵ Ergebnis des Abgleichs zweier Templates ist die Errechnung der Wahrscheinlichkeit der Übereinstimmung der verglichenen Personen.⁶⁶ Das Template

⁵⁷ BVerfGE 165, 363 (411 f. Rn. 107).

⁵⁸ Vgl. BVerfGE 165, 363 (411 f. Rn. 107).

⁵⁹ LT-Drs. 20/4284, S. 51 f.

⁶⁰ Siehe zuletzt zur Zulässigkeit dieser Eingriffsschwelle im Allgemeinen Polizei- und Sicherheitsrecht umfassend BayVerfGH, Entscheidung v. 13.3.2025 – Vf. 5-VIII-18 ua. = NVwZ 2025, 1599 f.

⁶¹ BVerfGE 165, 363 (398 f. Rn. 73).

⁶² BVerfGE 162, 1 (117 Rn. 248) m.w.N.

⁶³ Einen abschließenden Katalog dieser Rechtsgüter hat das BVerfG bislang nicht herausgebildet. Es spricht jedoch einiges dafür, dass die sexuelle Selbstbestimmung Teil dieser Rechtsgütergruppe ist, vgl. BVerfGE 156, 65 (144 f. Rn. 277) sowie DJB, Policy Paper: Sexualisierte Gewalt – Schutzlücken und Reformbedarfe, 18.11.2024, S. 7 f.

⁶⁴ Edpb, Leitlinien 05/2022 über den Einsatz von Gesichtserkennung im Bereich der Strafverfolgung, angenommen am 26.04.2023, abrufbar unter: https://www.edpb.europa.eu/system/files/2024-05/edpb_guidelines_202304_frtlawenforcement_v2_de.pdf (letzter Abruf 11.08.2026), S. 10.

⁶⁵ Ebd.

⁶⁶ Ebd. S.11.

ermöglicht einen Abgleich in hoher Geschwindigkeit und mit höherer Effizienz, als es bei einer menschlichen Durchsicht von Bildern möglich ist. Neben Gesichtern können z.B. auch Stimmen oder Gangmuster für einen solchen Abgleich genutzt werden.⁶⁷

Die Einführung von Befugnissen für biometrische Fernidentifizierung unterliegt Vorgaben des EU-Rechts, aber auch solchen des Verfassungsrechts.

Bei der biometrischen Fernidentifizierung handelt es sich um eine sowohl politisch als auch rechtlich umstrittene polizeirechtliche Maßnahme. Das Europäische Parlament wollte biometrische Echtzeit-Fernidentifizierung ursprünglich ohne die bestehenden Ausnahmen in der KI-VO verbieten. Der Europäische Datenschutzausschuss (EDSA) qualifizierte biometrische Fernidentifizierung in öffentlichen Räumen als eine Form der Massenüberwachung, welche Demokratien grundsätzlich fremd sei und hält eine Verarbeitung personenbezogener Daten in einer Datenbank durch „Scrapen“, z. B. von Bildern aus sozialen Netzwerken, für unionsrechtswidrig.⁶⁸ Andere in der wissenschaftlichen Literatur charakterisieren biometrische Fernidentifizierung aufgrund der lebenslangen Beständigkeit der Merkmale als eine der eingriffsintensivsten Maßnahmen, welche im digitalen Kontext möglich geworden seien,⁶⁹ oder verweisen darauf, dass durch sie die „Anonymität des Alltäglichen“ verschwinde.⁷⁰ Eine abschließende Beurteilung ist in dieser Stellungnahme nicht möglich.

IV. Echtzeit-Fernidentifizierung in öffentlich zugänglichen Räumen, §§ 184b, 184c LVwG-E

1. Erfordernis einer gesetzlichen Grundlage

Für eine rechtskonforme Nutzung biometrischer Echtzeit-Fernidentifizierung ist eine spezialgesetzliche Befugnis zum einen aufgrund des Art. 5 Abs. 5 KI-VO, zum anderen aufgrund des Gesetzesvorbehalts und der Wesentlichkeitstheorie im deutschen Verfassungsrecht geboten.⁷¹

⁶⁷ Vgl. hierzu ErwGr 15 KI-VO; zur Notwendigkeit der Beachtung der Rechtsprechung des Bundesverfassungsgerichts und den datenschutzrechtlichen Vorgaben trotz der Vorgaben der KI-VO, Coombe/Roth-Isigkeit, ZfDR 2024, 391 (413).

⁶⁸ Edpb, Leitlinien 05/2022 über den Einsatz von Gesichtserkennung im Bereich der Strafverfolgung, angenommen am 26.04.2023, abrufbar unter: https://www.edpb.europa.eu/system/files/2024-05/edpb_guidelines_202304_frlawenforcement_v2_de.pdf (letzter Abruf 11.08.2026), S. 34.

⁶⁹ Coombe/Roth-Isigkeit, ZfDR 2024, 391 (415).

⁷⁰ Martini, NVwZ 2022, 30 (31).

⁷¹ Siehe Auseinandersetzung bei Coombe/Roth-Isigkeit, ZfDR 2024, 391 (394); Zu den verfassungsrechtlichen Anforderungen an eine Rechtsgrundlage aus den Geboten der Bestimmtheit und Normenklarheit, siehe Hahn, Automatisierte Gesichtserkennung in der Strafverfolgung, 2025, S. 132-135. Zur Notwendigkeit einer expliziten Ermächtigungsgrundlage für grundrechtsrelevante staatliche Maßnahmen in „digitalen Kontexten“ vgl. auch Rachut, Grundrechtsverwirklichung in digitalen Kontexten, 2024, S. 205, 603 ff.

2. Sekundärrechtliche Vorgaben des Europarechts

Neben GRCh, EMRK und GG bestimmt insbesondere die KI-VO die Grenzen der Ausgestaltungsoptionen. Das „Verbot“ der Verwendung von Systemen zur Echtzeit-Fernidentifizierung in Art. 5 Abs. 1 lit. h KI-VO gilt gegenüber Art. 10 JI-RL als *lex specialis*.⁷² Nach der KI-VO bedarf eine Rechtsgrundlage über biometrische Echtzeit-Fernidentifizierung, als grundsätzlich verbotene und nur ausnahmsweise zulässige Praktik (Art. 5 Abs. 1 lit. h KI-VO), detaillierter Vorschriften zu Beantragung, Erteilung und Ausübung der Genehmigung, Beaufsichtigung, Berichterstattung und der Zulässigkeit der Maßnahme für die genannten Ziele (Art. 5 Abs. 5 S. 1, 2 KI-VO).

Gemäß Art. 6 Abs. 2 i.V.m. Anhang III Nr. 1 lit. a KI-VO unterliegt die biometrische Echtzeit-Fernidentifizierung als Hochrisiko-KI über die Erfüllung des Ausnahmetatbestandes des Art. 5 KI-VO hinaus außerdem einer Reihe an weiteren Anforderungen.⁷³ Diese umfassen unter anderem die Einrichtung eines Risikomanagementsystems (Art. 9 KI-VO), Daten und Daten-Governance (Art. 10 KI-VO), aber auch bspw. Anforderungen an Genauigkeit, Robustheit und Cybersicherheit (Art. 15 KI-VO). Hinzu kommen spezifische Betreiberpflichten, wie beispielsweise die Durchführung einer Grundrechtfolgenabschätzung (Art. 27 KI-VO).

Grundsätzlich gilt außerdem weiterhin das Regelungsregime der JI-RL, welches in den entsprechenden nationalen Normen umgesetzt wurde.⁷⁴

3. Verfassungsrechtliche Voraussetzungen

Angesichts des ausführlichen Rechtsrahmens der KI-VO kommt den verfassungsrechtlichen Wertungen insbesondere dann große Bedeutung zu, wenn biometrische Fernidentifizierung ohne KI im Sinne der KI-VO umgesetzt werden sollte und wenn trotz der KI-VO von einem nicht abschließend unionsrechtlich determinierten Bereich⁷⁵ ausgegangen werden kann.

Echtzeit-Fernidentifizierung war bisher nicht Gegenstand der Rechtsprechung des Bundesverfassungsgerichts. Zu ihrer Bewertung sind deshalb die im Rahmen anderer sicherheitsrechtlicher Maßnahmen entwickelten Grundsätze heranzuziehen. Biometrische

⁷² ErwGr 38f KI-VO., Hofmann-Coombe, EuR 2025, 363 (373); Leitlinien der Kommission zu verbotenen Praktiken der künstlichen Intelligenz gemäß der Verordnung (EU) 2024/1689 (KI-Verordnung), abrufbar unter: <https://digital-strategy.ec.europa.eu/de/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act> (letzter Abruf 11.08.2026), S. 18 Rn. 46.

⁷³ Raue, in: BeckOK KI-Recht, 3. Ed. 01.08.2025, Art. 5 KI-VO Rn. 114.

⁷⁴ Art. 2 Abs. 7 KI-VO, ErwGr 45 KI-VO; Leitlinien der Kommission zu verbotenen Praktiken der künstlichen Intelligenz gemäß der Verordnung (EU) 2024/1689 (KI-Verordnung), abrufbar unter: <https://digital-strategy.ec.europa.eu/de/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act> (letzter Abruf 11.08.2026), S. 18 Rn. 46.

⁷⁵ BVerfGE 152, 152 (Rn. 44 ff.)

Echtzeit-Fernidentifizierung stellt eine Kombination aus Videoüberwachung und Datenanalyse dar. Dies muss sich in der verfassungsrechtlichen Bewertung niederschlagen.⁷⁶

Die Technik greift in das Recht auf informationelle Selbstbestimmung ein. Die Erhebung,⁷⁷ die Speicherung⁷⁸ und der Abgleich sind als eigenständige Eingriffe, auch im Nichttrefferfall, zu qualifizieren.⁷⁹ Hahn geht zudem von einem Eingriff durch die Erstellung des Templates aus.⁸⁰ Bei der Bewertung der Eingriffsintensität des Abgleichs ist zum einen die vorgelagerte Maßnahme der Datengewinnung zu berücksichtigen, zum anderen kommt es auf die Ausgestaltung der Datenverarbeitung an.⁸¹

Wird eine hohe Anzahl Betroffener, welche durch ihr Verhalten keinen Anlass zu einer Überwachung gegeben haben, erfasst, wirkt sich das eingriffsintensivierend auf die Maßnahme aus.⁸² Der Eingriff entfällt nicht dadurch, dass sich die Beteiligten im öffentlichen Raum aufhalten, auch bei Kenntnis nicht.⁸³ Indem der Entwurf auf § 184 Abs. 1 und 3 LVwG-E, nicht aber auf § 184 Abs. 7 LVwG-E verweist,⁸⁴ wirft er die Frage auf, ob keine Durchführung erlaubt ist, wenn Dritte unvermeidbar von den Aufnahmen betroffen sind. Damit wäre aber mangels Umsetzbarkeit die Sinnhaftigkeit der Maßnahme insgesamt in Frage gestellt. Lehnt man eine solche Einschränkung dementsprechend ab, weist die Maßnahme eine hohe Streubreite auf. Dann ist anzunehmen, dass die Aufnahmen eine Vielzahl Unbeteiligter erfassen, welche selbst keinerlei Anlass gesetzt haben.

Hinsichtlich der Datenverarbeitung ist zu berücksichtigen, dass biometrische Merkmale unveränderlich sind und damit sehr sensibel und hier deshalb eine hohe Missbrauchsanfälligkeit besteht.⁸⁵ Bei privater Software kommt die Gefahr unbemerkter Manipulation und des unbemerkten Datenzugriffs hinzu.⁸⁶ Eine Rolle spielt auch, dass für Unbeteiligte das Risiko besteht, zum Ziel weiterer Maßnahmen zu werden.⁸⁷ Zwar kann der Einsatz selbstlernender Systeme aufgrund der mangelnden Nachvollziehbarkeit das Eingriffsgewicht erhöhen.⁸⁸ Dies kann nach dem BVerfG aber auch für deterministische Modelle

⁷⁶ Coombe/Roth-Isigkeit, ZfDR 2024, 391 (394).

⁷⁷ BVerfGE 130, 151 (184); Hahn, Automatisierte Gesichtserkennung in der Strafverfolgung, 2025, S. 98; Schindler, Biometrische Videoüberwachung, 2021, S. 310.

⁷⁸ BVerfGE 130, 151 (184); Hahn, Automatisierte Gesichtserkennung in der Strafverfolgung, 2025, S. 98; Schindler, Biometrische Videoüberwachung, 2021, S. 310.

⁷⁹ BVerfGE 150 (244); Hahn, Automatisierte Gesichtserkennung in der Strafverfolgung, 2025, S. 101; Schindler, Biometrische Videoüberwachung, 2021, S. 305 ff.; Ogorek, LTZ 2024, 274 (278); Martini, NVwZ-Extra 2022, 1 (6).

⁸⁰ Hahn, Automatisierte Gesichtserkennung in der Strafverfolgung, 2025, S. 99; a.A. Schindler, der dies unter die Bereitstellung des Referenzmaterials fasst. Schindler, Biometrische Videoüberwachung, 2021, S. 314 f.

⁸¹ BVerfGE 165, 363 (390).

⁸² Zur automatisierten Kennzeichenkontrolle BVerfGE 150, 244 (283).

⁸³ BVerfG NVwZ 2007, 688 (690).

⁸⁴ § 184b Abs. 1 S. 1 LVwG-E.

⁸⁵ Zur Vertiefung des Eingriffsgewichts durch Missbrauchsgefahr BVerfGE 165, 363 (399 Rn. 76).

⁸⁶ BVerfGE 165, 363 (408 Rn. 100).

⁸⁷ BVerfGE 165, 363 (400 Rn. 77).

⁸⁸ BVerfGE 165, 363 (408 Rn. 100).

gelten.⁸⁹ Zusätzlich sind die Fehleranfälligkeit der Technik⁹⁰ und die der Technik innewohnende Diskriminierungsproblematik⁹¹ aus verfassungsrechtlicher Perspektive problematisch. Zum einen kann die Technik selbst,⁹² zum anderen die Interaktion der Menschen mit der Technik⁹³ diskriminierend sein.

Erschwerend wirken außerdem mögliche Einschüchterungseffekte.⁹⁴ Gerade der Aspekt der Einschüchterung betrifft nicht nur die betroffene Person, sondern kann nachteilige Auswirkungen auf das freiheitlich demokratische Gemeinwesen insgesamt mit sich bringen.⁹⁵

Zusammenfassend ist bei der biometrischen Echtzeit-Fernidentifizierung sowohl mit als auch ohne KI von einer sehr hohen Eingriffsintensität auszugehen. Damit unterliegt eine verfassungsrechtliche Rechtfertigung der Maßnahme hohen Hürden.

4. Einzelne Aspekte der Norm

Die nachfolgende Auseinandersetzung fokussiert sich auf einige besonders hervorzuhebende Aspekte der geplanten Norm.

a) Gemeinsame Einsatzbedingungen von Systemen mit und ohne Qualifikation als KI-System i.S.d. KI-VO

Begrüßenswert ist, dass im Gesetzesentwurf nicht mehr zwischen biometrischer Echtzeitfernidentifizierung unter Einsatz von Künstlicher Intelligenz und biometrischer Echtzeitfernidentifizierung unter Verwendung von Systemen, welche nicht als Künstliche Intelligenz im Sinne der KI-VO zu qualifizieren sind, unterschieden wird. Ausdrücklich erklärt § 184b Abs. 1 S. 5 LVwG-E, dass § 184b Abs. 1 S. 1-4 LVwG-E auch bei einer Anwendung, welche keine Künstliche Intelligenz im Sinne der KI-VO darstellt, Geltung beanspruchen.

In Anbetracht der weiten Definition der KI-VO wäre fraglich, ob ein tatsächlicher Anwendungsbereich für Systeme verbliebe, die nicht als KI im Sinne der KI-VO eingeordnet werden können.⁹⁶ Das gilt insbesondere vor dem Hintergrund, dass aufgrund des ähnlichen Gefährdungspotenzials vertreten wird, der KI-Begriff in Art. 3 Nr. 1 KI-VO sei weit

⁸⁹ BVerfGE 165, 363 (409 Rn. 101).

⁹⁰ BVerfGE 165, 363 (409 Rn. 102).

⁹¹ Zum Problem der Diskriminierung bei selbstlernenden Systemen BVerfGE 165, 363 (408 Rn. 100).

⁹² Buolamwini/Gebru, *Proceedings of Machine Learning Research* (81) 2018, 1.

⁹³ Alon-Barkat/ Busuioc, *Journal of Public Administration Research and Theory* (33) 2023, 153.

⁹⁴ Zur automatisierten Kennzeichenkontrolle „Gefühl des Überwachtwerdens“ BVerfGE 150, 244 (283).

⁹⁵ BVerfGE 115, 320, (354 f).

⁹⁶ Nach Wendehorst sprechen teleologische Erwägungen für ein weites Begriffsverständnis. Wendehorst in: Martini/Wendehorst, *KI-VO*, 1. Aufl. 2024, Art. 3 Rn. 6. Töpfer/Kleemann gehen z.B. davon aus, dass moderne Gesichtserkennungssysteme unter die KI-VO fallen. Töpfer/Kleemann, *Polizeiliche Gesichtserkennung*, Deutsches Institut für Menschenrechte 2025, S. 18.

auszulegen und auch komplexe regelbasierte Systeme würden unter die KI-VO fallen.⁹⁷ Angesichts der begrifflichen Auslegungsschwierigkeiten im Rahmen der KI-VO entstünde durch eine Unterscheidung für die anwendende Behörde eine vermeidbare Rechtsunsicherheit.⁹⁸

b) Vier-Augen-Prinzip und Qualifikation der Zugangsberechtigten

Die Grenzen der menschlichen Fähigkeit zur Überprüfung von Entscheidungen durch KI sind ebenso umstritten wie die Frage nach dem Gelingen einer wirksamen Aufsicht.⁹⁹ Diese zwei Aspekte werden in der KI-VO geregelt, stellen aber auch bedeutsame Gesichtspunkte im Rahmen der verfassungsrechtlichen Wertung dar, da sie in Bezug zur Fehleranfälligkeit der Technik und möglichen Diskriminierungen stehen. Dementsprechend wichtig und positiv zu werten ist, dass § 184c Abs. 1 S. 2 LVwG-E nun eine Überprüfung und Bestätigung des Ergebnisses des Abgleichs durch zwei qualifizierte Beschäftigte der Polizei vorschreibt, bevor weitere Maßnahmen getroffen werden.

Als eine Bedingung schreibt die KI-VO in Art. 14 Abs. 5 KI-VO für Hochrisiko-KI-Systeme nach Anhang III Nr. 1 lit. a KI-VO vor, dass Ergebnisse eines Identifizierungsvorgangs getrennt von **zwei natürlichen Personen**, welche über die notwendige Kompetenz, Ausbildung und Befugnis verfügen, überprüft werden müssen. Zwar ist eine Ausnahme von der Prüfung durch zwei natürliche Personen im hier betroffenen Bereich¹⁰⁰ aufgrund Unverhältnismäßigkeit gemäß Art. 14 Abs. 5 UAbs. 2 KI-VO möglich. Angesichts der gravierenden Auswirkungen einer fehlerhaften Identifizierung, des Beruhens des Ergebnisses auf einer Wahrscheinlichkeitsrechnung sowie der höheren Fehlerrate bei Aufnahmen schlechter Qualität¹⁰¹ sollte aber nicht vom Vier-Augen-Prinzip abgewichen werden.¹⁰² Zustimmungswürdig ist daher, dass nach dem Entwurf ein solches Abweichen nicht ermöglicht wird. Die hinreichende Qualifizierung der Beamten ist unabhängig von der Vorgabe in der KI-VO auch wegen der eingeschränkten menschlichen Kompetenzen bei der Erkennung von Gesichtern bedeutsam.¹⁰³ Entsprechend begrüßenswert sind die diesbezüglichen Vorgaben in § 184c Abs. 1 S. 2 und Abs. 3 LVwG-E.

⁹⁷ So unter Verweis auf das Regelungsziel und die vielfachen Sondervorschriften, Hofmann-Coombe, EuR 2025, 363 (370); Krönke, NVwZ 2024, 529 (529 f.), Wendehorst, in: Martini/Wendehorst, KI-VO, 1. Aufl. 2024, Art. 3 Rn. 6.

⁹⁸ Dies erkennt der Entwurf zutreffend an. Siehe Entwurf, S. 45.

⁹⁹ Laux/Langer/Baum, Wie menschliche Aufsicht über Künstliche Intelligenz gelingt, FAZ vom 08.10.2025.

¹⁰⁰ Nach der Definition in Art. 3 Nr. 46 KI-VO erfasst die Strafverfolgung auch die Gefahrenabwehr.

¹⁰¹ Hahn, Automatisierte Gesichtserkennung in der Strafverfolgung, 2025, S. 55; zu Problemen der Richtigkeitsgewähr, siehe auch Martini/Kemper mit Nachweisen in den Fußnoten, CR 2023, 341 (343) Fn. 41-44.

¹⁰² Entsprechend für die Strafverfolgung und Identifizierungsverfahren Hahn, Automatisierte Gesichtserkennung in der Strafverfolgung, 2025, S. 310.

¹⁰³ Hahn fordert für den Einsatz in Strafverfahren wegen der eingeschränkten menschlichen Kompetenzen zur Gesichtserkennung eine Überprüfung durch ausgebildete Lichtbildsachverständige, siehe Hahn, Automatisierte Gesichtserkennung in der Strafverfolgung, 2025, S. 309; zu den Grenzen der menschlichen Fähigkeiten zur Gesichtserkennung mit weiteren Nachweisen, siehe Schindler, Biometrische Videoüberwachung, 2021, S. 121. Studien zu Co-Kreation deuten außerdem darauf hin, dass im Zusammenwirken von

c) Prinzip der Normenklarheit

Durch die Vielzahl an Verweisungen in der Norm wird das Normverständnis und damit die rechtskonforme Anwendung erschwert.

In § 184b LVwG-E wird neunmal auf Bestimmungen der KI-VO verwiesen. Soweit aus dem Verordnungsentwurf ersichtlich, ist Hintergrund der Verweisungstaktik das europarechtliche Normwiederholungsverbot.¹⁰⁴ Das Normwiederholungsverbot gilt jedoch nicht uneingeschränkt. So erkannte der EuGH an, dass im Sinne der Verständlichkeit die Wiederholung bestimmter Punkte einer Verordnung möglich ist, wenn nationale und europarechtliche Normen zusammenspielen.¹⁰⁵ Art. 5 Abs. 5 KI-VO ermächtigt zum Erlass nationaler Vorschriften und ermöglicht dabei auch strengere Voraussetzungen als die in der KI-VO enthaltenen (Art. 5 Abs. 5 S. 5 KI-VO). Zudem ist eine konkrete nationale Bestimmung hinsichtlich einiger Aspekte erforderlich (Art. 5 Abs. 5 S. 2, 3 KI-VO). Aufgrund des Prinzips der Normenklarheit wäre es empfehlenswert, mit weniger Verweisungen auf die KI-VO zu arbeiten, um eine bessere Verständlichkeit der Vorschrift für Rechtsanwender und Betroffene zu bewirken.

V. Nachträgliche Fernidentifizierung unter Einbeziehung von Bildern aus dem Internet gem. §§ 195b, 195c LVwG-E

1. Erfordernis einer gesetzlichen Grundlage

Auch hinsichtlich der nachträglichen Fernidentifizierung ist die Einführung einer speziellen Ermächtigungsgrundlage verfassungsrechtlich geboten, um eine solche rechtmäßig durchführen zu können. Überdies ergibt sich die Notwendigkeit aus Art. 8 Abs. 2 JI-RL.¹⁰⁶

2. Verbot des Art. 5 Abs. 1 lit. e KI-VO

Die für §§ 195b, 195c LVwG-E in Frage kommenden Systeme sind nach dem technischen Stand aller Wahrscheinlichkeit nach von dem Verbot des Art. 5 Abs. 1 lit. e KI-VO erfasst. Die Norm ordnet „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“, den verbotenen Praktiken im KI-Bereich zu. Der Abgleich von biometrischen Referenzdaten Daten zu Stimmen oder Gesichtern, welche die Polizei im Rahmen ihrer Aufgaben erhalten und verarbeitet hat (§ 195b Abs. 1 S. 2 LVwG-E), mit

Menschen und KI oftmals schlechtere Ergebnisse erzielt werden. Bessere Ergebnisse werden nur bei hoher Expertise der beteiligten Personen erzielt, siehe Vaccaro et. al, Nature Human Behaviour (8) 2024, 2293.

¹⁰⁴ Entwurf, S. 44.

¹⁰⁵ EuGH 28.03.1983 – 272/83, LMRR 1983, 49 Rn. 27; siehe auch Lauber/Rönsberg in: Specht/Mantz, Hdb Europäisches und deutsches Datenschutzrecht, 1. Aufl. 2019, § 4 BSDG Rn. 15, 16.

¹⁰⁶ Hahn, Automatisierte Gesichtserkennung in der Strafverfolgung, 2025, S. 202. Die JI-RL ist gemäß Art 26 Abs. 10 UAbs. 4 KI-VO weiterhin anwendbar, siehe Eisenberger in: Martini/Wendehorst, KI-VO, 1. Aufl. 2024, Art. 26 Rn. 62; Coombe/Roth-Isigkeit, ZfDR 2024, 391 (410).

biometrischen Vergleichsdaten, welche sie für den Abgleich aus dem Internet mittels einer automatisierten Anwendung verarbeitet hat (§ 195b Abs. 1 S. 3 LVwG-E), ist damit europarechtlich problematisch.

Im Einzelnen ist noch nicht geklärt, was ein ungezieltes Auslesen von einem gezielten Auslesen unterscheidet. Der vorliegende Entwurf geht davon aus, dass das Kriterium „ungezieltes Auslesen“ nicht erfüllt sei, wenn die Gesichtsbilder anlassbezogen erhoben und verarbeitet werden und nicht für zukünftige Verwendung in Datenbanken gespeichert werden.¹⁰⁷ Demgegenüber legen die (unverbindlichen) Leitlinien der Kommission „ungezielt“ dahingehend aus, dass bei dem Auslesen kein Schwerpunkt auf bestimmte Personen oder Gruppen gelegt wird.¹⁰⁸ Nach den Leitlinien ist ungezieltes Auslesen auch dann gegeben, wenn nur bestimmte Gruppen betroffen sind, sofern das Ergebnis funktional dem der verbotenen Praktik entspricht.¹⁰⁹ Im Einklang mit dem Gesetzesentwurf hält die Kommission trotz dieser funktionalen Interpretation eine Reverse-Engineering-Technologie zur Suche nach einem Bild im Internet für ein gezieltes Auslesen.¹¹⁰

Nach derzeitigem Stand ist die technische Umsetzbarkeit eines Abgleichs mit öffentlich zugänglichen Daten aus dem Internet ohne den Aufbau einer Datenbank aber nicht möglich.¹¹¹ Legt man die Rechtsauffassung der Kommission zu Grunde, würden auch temporäre und dezentrale Datenbanken dem Verbot unterfallen.¹¹² Somit könnte eine europarechtskonforme Umsetzung des §195b LVwG-E derzeit technisch unmöglich sein.

Insoweit der Entwurf zum Abgleich anderer biometrische Daten, wie Stimmen, ermächtigt, ist kein Verstoß gegen Art. 5 Abs. 1 lit. e KI-VO anzunehmen, ebenso wenig, sofern kein KI-System verwendet wird.¹¹³ In diesen Fällen sind die Anforderungen an Hochrisiko-KI und Vorgaben der JI-RL (in Form ihrer landesrechtlichen Umsetzungsnormen) zu beachten.

¹⁰⁷ Entwurf, S. 59.

¹⁰⁸ Siehe zur Einordnung (unverbindlich): Leitlinien der Kommission zu verbotenen Praktiken der künstlichen Intelligenz gemäß der Verordnung (EU) 2024/1689 (KI-Verordnung), abrufbar unter: <https://digital-strategy.ec.europa.eu/de/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act> (letzter Abruf 11.08.2026), S. 93 Rn. 228.

¹⁰⁹ Ebd. S. 94 Rn. 230.

¹¹⁰ Ebd. S. 94 Rn. 233.

¹¹¹ Lewandowski, Technisches Gutachten: Braucht die Polizei eine Datenbank zum biometrischen Abgleich?, September 2025, abrufbar unter: <https://algorithmwatch.org/de/gutachten-datenbank-biometrie-gesichtserkennung/> (letzter Abruf 11.08.2026); Stellungnahme BFDI, Ausschuss für Inneres und Heimat, Ausschuss-Ds. 20(4)483, abrufbar unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Stellungnahmen/2024/StgN_Innere-Sicherheit-Asylsystem-Gesetz.html (letzter Abruf 11.08.2026); siehe auch Rückert, StV 2025, 350 (353).

¹¹² Leitlinien der Kommission zu verbotenen Praktiken der künstlichen Intelligenz gemäß der Verordnung (EU) 2024/1689 (KI-Verordnung), abrufbar unter: <https://digital-strategy.ec.europa.eu/de/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act> (letzter Abruf 11.08.2026), S. 93 Rn. 226.

¹¹³ Ebd. S. 95 Rn. 234.

3. Gleichwertigkeit der Eingriffstiefe durch nachträgliche Fernidentifizierung gegenüber der Echtzeit-Fernidentifizierung

Bereits im Zuge der KI-VO war die Unterscheidung in Echtzeit-Fernidentifizierung und retrograde Fernidentifizierung kritisiert worden.¹¹⁴ Vor dem Hintergrund, dass nachträgliche biometrische Fernidentifizierung auch eine Profilbildung ermöglicht, wurde von manchen sogar ein - gegenüber der Durchführung in Echtzeit mit sofortiger Löschung - tieferer Grundrechtseingriff angenommen.¹¹⁵ Dies gilt es zu überdenken.

4. Verfassungsrechtliche Bedenken

Eine besonders starke Rolle kommt dem Verfassungsrecht für die nicht von dem Verbot erfassten Fälle zu.

Ungeachtet des Verbotes von Art. 5 Abs. 1 lit. e KI-VO ist aus verfassungsrechtlicher Perspektive die Ähnlichkeit einer solchen Datenbank zur Vorratsdatenspeicherung¹¹⁶ anzumerken. Mit dem Unterschied, dass nicht nur personenbezogene, sondern noch sensiblere Daten¹¹⁷ gespeichert werden würden. Dementsprechend höher ist das potenzielle Missbrauchsrisiko.

Zudem ist die Maßnahme aus weiteren verfassungsrechtlichen Gründen kritisch zu betrachten.

Ausweislich des Entwurfs erfasst der Abgleich sämtliche Daten, die zu diesem Zweck aus dem Internet erlangt wurden, auch Daten sozialer Medien, sofern sie sich nicht nur an einen abgegrenzten Personenkreis richten.¹¹⁸ Wie im Entwurf zutreffend beschrieben, liegt hierin die Anlasslosigkeit der Maßnahme sowie deren große Streubreite begründet. Auch erkennt der Entwurf zutreffend an, dass die Begrenzung auf öffentliche Daten keine andere Bewertung rechtfertigt. Die öffentliche Verfügbarkeit der personenbezogenen Daten im Internet lässt noch nicht auf die Zurverfügungstellung der betroffenen Personen schließen.¹¹⁹ Die Informationen können sowohl rechtswidrig von Dritten eingestellt worden sein, ohne dass die betroffene Person je hiervon erfährt, als auch durch die Personen

¹¹⁴Vaele/Bogesius, CRi 04/2021, 97 (101); Hahn hält nachträgliche Fernidentifizierung in bestimmten Situationen sogar für eingriffsintensiver, siehe Hahn, ZfDR 2023, 142 (154 ff.); in diese Richtung auch Coombe/Roth-Isigkeit, ZfDR 2024, 391 (410 f.).

¹¹⁵ Coombe/Roth-Isigkeit, ZfDR 2024, 391 (411).

¹¹⁶ Übersicht zur diesbezüglichen Rechtsprechung bei Sodan in: Sodan GG, Art. 10 GG, Rn. 14a, 14b; Bzgl. Clearview AI Kemper/Martini, CR 2023, 414 (417).

¹¹⁷ Nach Art. 10 JI-RL zählen biometrische Merkmale zu den besonderen Kategorien personenbezogener Daten für deren Verarbeitung höhere Standards gelten. Zur eingriffsmildernden Wirkung des Ausschlusses biometrischer Merkmale, BVerfGE 165, 363 (404 Rn. 87).

¹¹⁸ Entwurf, S. 58.

¹¹⁹ So auch die europäische Kommission, siehe (unverbindliche) Leitlinien der Kommission zu verbotenen Praktiken der künstlichen Intelligenz gemäß der Verordnung (EU) 2024/1689 (KI-Verordnung), abrufbar unter: <https://digital-strategy.ec.europa.eu/de/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act> (letzter Abruf 11.08.2026), S. 94 Rn. 232.

selbst, ohne Kenntnis der neuen Verarbeitungsmethoden. Hinzu kommt, dass die Daten nicht zum Zwecke eines solchen Abgleichs preisgegeben wurden.¹²⁰

Die Maßnahme birgt durch Falschidentifizierung außerdem das Risiko, dass Unbeteiligte Ziel von weiteren polizeilichen Eingriffen werden. Fehlerhaftigkeit und Diskriminierungsanfälligkeit der Systeme kommen je nach konkret verwendetem System eingriffsvertiefend hinzu.

Durch den Kontext der im Internet für den Abgleich gewonnenen Daten sind Rückschlüsse auf besuchte Veranstaltungen, ausgeübte Berufe und private Interessen,¹²¹ Erkenntnisse von Freizeitgewohnheiten bis hin zur religiösen Überzeugung¹²² möglich. Vor diesem Hintergrund positiv ist die Aufnahme von Vorschriften zum Kernbereichsschutz in § 195b Abs. 4 LVwG-E und die Beschränkung der Verwendung auf die Bestätigung der Identität einer Person gemäß § 195b Abs. 1 S. 1 LVwG-E.

Da es sich nichtsdestotrotz um einen schweren Eingriff in das Recht auf informationelle Selbstbestimmung handelt, ließe sich dieser verfassungsrechtlich, wenn überhaupt, nur unter strengsten Bedingungen rechtfertigen. Ob eine Übertragung der im Urteil des BVerfG zu HessenData dargestellten Grundsätze und, wie im Entwurf angenommen, der Rasterfahndung¹²³ ausreicht, ist angesichts der umfassenderen Zahl an betroffenen Personen und der hohen Sensibilität der Daten fraglich.

5. Zwischenfazit

Trotz der sichtlichen Bemühungen um eine Begrenzung der Maßnahme bestehen tiefgreifende europa- und verfassungsrechtliche Bedenken.

6. Einzelne Aspekte der Norm

Sollte dennoch an der Einführung der §§ 195b, 195c LVwG-E festgehalten werden, wird im Folgenden auf zwei Aspekte vertiefend eingegangen:

a) Gemeinsame Einsatzbedingungen von Systemen mit und ohne Qualifikation als KI-System i.S.d. KI-VO

Aus den oben genannten Gründen wäre die Unterscheidung in eine Durchführung unter Anwendung von Systemen mit und ohne KI nicht zielführend. Der gegenüber dem Referentenentwurf geänderte einheitliche Ansatz in der Normierung ist zu befürworten.

¹²⁰ Mit dieser Argumentation plädierten Martini und Kemper auch für eine teleologische Reduktion des Art. 9 Abs. 2 lit. e DSGVO. Martini/Kemper, CR 2023, 341 (347).

¹²¹ Martini/ Kemper, CR 2023, 341 (344).

¹²² Martini/ Kemper, CR 2023, 341 (345).

¹²³ Entwurf, S. 54.

b) Vier-Augen-Prinzip und Qualifizierung der Zugangsberechtigten

Begrüßenswert ist, dass auch in § 195c Abs. 1 S. 2 LVwG-E eine Überprüfung und Bestätigung durch zwei Beschäftigte der Polizei gefordert wird. Positiv ist auch die Beschränkung des Zugangs zu der Anwendung auf entsprechend qualifizierte Beschäftigte gemäß § 195c Abs. 3 S. 1 LVwG-E. Wie im Rahmen von §§ 184b, 184c LVwG-E sollte eine besondere Qualifikation nicht nur für die anwendenden, sondern auch für die überprüfenden Polizeibeamten/innen festgeschrieben werden.

VI. Abschließende Bemerkungen

1. Digitale Souveränität

Ein Problem, welches im Gesetzesentwurf keine Beachtung findet, ist die Sicherstellung der Datenhoheit und damit verbundenen wirksamen Vorbeugung von Missbrauch.¹²⁴ Die technikneutrale Formulierung der Vorschriften erlaubt den Einsatz zahlreicher, auch als problematisch wahrgenommener, privater¹²⁵ Software-Lösungen. Sollte dies beabsichtigt sein, empfiehlt sich die Implementierung einer dauerhaften technischen Analyse bzgl. der Zugriffs- und Missbrauchsmöglichkeiten des Softwareanbieters.¹²⁶ Angesichts der Sensibilität von biometrischen Merkmalen und der Fähigkeit umfangreicher Profilbildung sollte hier dringend nachgebessert werden.

2. Totalüberwachungsverbot

Das hohe Eingriffsgewicht und die damit verbundenen umfassenden Erkenntnismöglichkeiten durch die neuen Befugnisse der Polizei nötigen zu einem Blick auf das Totalüberwachungsverbot: Die automatisierte Datenanalyse ist in Einzelfällen fähig, insb. bei Personen, über die größere Datenmengen im polizeilichen Informationsverbund gespeichert sind, umfassende Persönlichkeitsprofile über Betroffene zu erzeugen.¹²⁷ Dies begründet die Gefahr eines Verstoßes gegen Art. 1 Abs. 1 GG in Form des Totalüberwachungsverbots.¹²⁸ Insbesondere die Variante des § 188c Abs. 4 LVwG-E weist diese Gefahr auf, da nicht nur Profilbildungen ausdrücklich zulässig sind, sondern zusätzlich keine zeitliche Begrenzungen des Datenmaterials greift und Daten aus besonders schweren Informationseingriffen wie der Online-Durchsuchung einbezogen werden können, die schon für

¹²⁴ Vgl. grundlegend zur digitalen Souveränität von Sicherheitsbehörden und Nachrichtendiensten Kelber/Bortnikov, NJW 2023, 2000 ff.; spezifisch zum Missbrauchspotential privater Software BVerfGE 165, 363 (408 Rn. 100) sowie Wissenschaftlicher Dienst des Deutschen Bundestags, Datenbank-Analysen durch die Polizei. Grundrechte und Datenschutzrecht, 2. März 2020, WD3-3000-018/20, S. 8 m.w.N.

¹²⁵ Siehe hierzu die aktuelle Debatte um den Einsatz von Softwarelösungen von Palantir Technologies.

¹²⁶ Santhakumar, in: Botta et al., Rechtsfragen virtueller Welten, 2025, S. 103 (114 f.).

¹²⁷ BVerfGE 165, 363 (430 Rn. 150): Die Rechtsgrundlagen für automatisierte Datenanalyse eignen sich „in ihrer daten- und methodenoffenen Unbegrenztheit [...] mit einem Klick umfassende Profile von Personen“ zu erstellen.

¹²⁸ Siehe umfassend zum Totalüberwachungsverbot bei Ziegler, RW 2024, 374 ff.; Eichberger, in: Huber/Voßkuhle, 8. Aufl. 2024, GG Art. 2 Rn. 315 ff.

sich genommen eine Gefahr zur Bildung eines umfassenden Persönlichkeitsprofils aufweist.¹²⁹

Demgegenüber positiv ist der Ausschluss der Weiterverarbeitung von Daten aus der Maßnahme der biometrischen Echtzeit-Fernidentifizierung in § 184c Abs. 1 S. 1 Hs. 2 LVwG-E und der nachträglichen Fernidentifizierung in § 195c Abs. 1 S. 1 Hs. 2 LVwG-E. Damit wird die Gefahr, dass aus der Maßnahme erlangte Erkenntnisse im Rahmen der Datenweiterverarbeitung zur Bildung umfassender Persönlichkeitsprofile beitragen könnten, adressiert.¹³⁰

Vor diesem Hintergrund außerdem zu begrüßen ist die bereits bestehende Regelung in § 186a Abs. 8 LVwG. Als verfahrensrechtliche Absicherung zur Verhinderung der Bildung umfassender Persönlichkeitsprofile reicht diese bloße Wiederholung des Totalüberwachungsverbots jedoch nicht aus.¹³¹

3. Transparenz und Rechtsschutz

Die Frage transparenten Handelns von Sicherheitsbehörden „ist [...] nicht nur eine Frage politischer Opportunität“¹³², sondern eine fundamentale Anforderung im demokratischen Rechtsstaat. Da es sich bei der Datenanalyse und der biometrischen Fernidentifizierung um besonders eingriffsintensive Maßnahmen handelt, die teilweise unter den gleichen Voraussetzungen stehen wie heimliche Überwachungsmaßnahmen, böte sich zur Überprüfung der Wirksamkeit sowie zur Steigerung der Legitimation und des Vertrauens in eine rechtsstaatliche Handhabung der Maßnahmen an,¹³³ Transparenz- und Berichtsvorschriften einzufügen.

Begrüßenswert ist insofern, dass § 184c Abs. 3 S. 3 LVwG-E auf die Berichtspflicht in Art. 5 Abs. 4 KI-VO verweist und damit die Vorgaben der KI-VO zur Mitteilung jeder Verwendung eines biometrischen Echtzeit-Fernidentifizierungssystems in öffentlich zugänglichen Räumen an die zuständige Marktüberwachungsbehörde und die nationalen Datenschutzbehörden umsetzt. Gemäß Art. 5 Abs. 7 KI-VO werden Jahresberichte über die Verwendung biometrischer Echtzeitfernidentifizierungssysteme in öffentlich zugänglichen Räumen, die auf aggregierten Daten der Mitgliedstaaten beruhen, durch die Kommission veröffentlicht. Eine ähnliche, etwas weniger strenge Berichtspflicht findet sich auch in § 195c Abs. 3 S. 3 HS. 2 LVwG-E, Art. 26 Abs. 10 UAbs. 6 KI-VO. Auch die Verankerung der Protokollpflichten für biometrische Echtzeit-Fernidentifizierung und nachträgliche Fernidentifizierung in § 186c LVwG-E leistet in Verbindung mit § 186b Abs. 1 und 2 LVwG-

¹²⁹ Ziegler, in: Botta et al., Rechtsfragen virtueller Welten, 2025, S. 85 (99); Ziegler, RW 2024, 374 (398).

¹³⁰ Differenziert nach biometrischer Fernidentifizierung im öffentlichen Raum und im Internet Ziegler, in: Botta et al., Rechtsfragen virtueller Welten, 2025, S. 85 (97 ff.).

¹³¹ Ziegler, RW 2024, 374 (397 f., insb. Fn. 168).

¹³² MPI, Überwachungsgesamtrechnung für Deutschland, Bd. I, 2025, S. 16.

¹³³ MPI, Überwachungsgesamtrechnung für Deutschland, Bd. I, 2025, S. 20.

E durch Stichproben des Landesbeauftragten für Datenschutz und dort normierte Berichtspflichten einen Beitrag zur Transparenz.

4. Evaluation

Wegen der unklaren Effektivität biometrischer Überwachung, der Datenanalyse und der Eingriffsintensität dieser Maßnahmen, sowie der möglichen Einschüchterungseffekte, wird zudem empfohlen, Evaluierungsvorschriften aufzunehmen.

5. Fazit und abschließende Handlungsempfehlungen

Der Entwurf eines Gesetzes zur Fortentwicklung polizeirechtlicher Maßnahmen für einen wirksamen Schutz der öffentlichen Sicherheit ist ambitioniert. Er hat das Ziel, der Zunahme bestimmter Kriminalitätsformen durch neue bzw. erweiterte Befugnisse der Polizei zu begegnen. Ob dies wirksam sein wird, ist hier nicht zu beurteilen. Soweit es die in dieser Stellungnahme adressierten Vorschriften betrifft, besteht aus verfassungsrechtlicher und auch gesetzessystematischer Sicht Änderungsbedarf. Dieser kann wie folgt zusammengefasst werden:

- § 184b LVwG-E sollte aus Gründen der Normenklarheit weniger Verweisungen in die KI-VO vornehmen.
- § 186a Abs. 8 LVwG-E sollte bei der Gelegenheit der Änderung des LVwG zu einer verfahrensrechtlichen Sicherung gegen die Erstellung umfassender Persönlichkeitsprofile ausgebaut werden.
- Die Erlaubnis zur Profilbildung im Rahmen der Datenanalyse mittlerer Schwere (§ 188c Abs. 3 LVwG-E) sollte ersatzlos gestrichen werden, da sie verfassungswidrig ist.
- Die nachträgliche biometrische Fernidentifizierung unter Einschluss von aus dem Internet gewonnenen Daten in §§ 195b, 195c LVwG-E sollte ersatzlos gestrichen werden, da erhebliche verfassungs- und europarechtliche Bedenken gegen sie bestehen. Sollte entgegen unserer Empfehlung daran festgehalten werden, wäre die Anforderung einer besonderen Qualifikation der überprüfenden Beamten vorzusehen.
- Abschließend empfiehlt sich die Einführung von Evaluierungsvorschriften zur evidenzbasierten Überprüfung der Effektivität und Wirksamkeit der neuen eingriffsintensiven Maßnahmen sowie Vorschriften zur digitalen Souveränität, um den Risiken des Einsatzes privater Software zu begegnen.