

gubitz⁺partner + Dänische Straße 15 + 24103 Kiel

Schleswig-Holsteinischer Landtag
z. Hd. Jan Kürschner,
Vorsitzender des Innen und Rechtsausschusses
Düsternbrooker Weg 70
24105 Kiel

Bei Antwort bitte stets angeben:
X-9189/21-MG MG

Bearbeiter:in
Prof. Dr. Gubitz

Kiel, den
10. September 2026

Stellungnahme zum Entwurf eines Gesetzes zur Fortentwicklung polizeirechtlicher Maßnahmen für einen wirksamen Schutz der öffentlichen Sicherheit (Drucks. 20/4284) und zum Änderungsantrag der Fraktionen von CDU und BÜNDNIS 90/Die GRÜNEN zu Drucksache 20/4284 (Umdruck 20/6786)

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

ich bedanke mich für die Gelegenheit zur Stellungnahme. Aufgrund des Gesamtumfangs und der erheblichen Anzahl neu vorgesehener Befugnisse und vor dem Hintergrund meiner beruflichen Expertise beschränkt sich die nachfolgende Stellungnahme auf einzelne ausgewählte Aspekte.

Vorab ein Überblick über die wesentlichen Kritikpunkte an den Neuregelungen:

- **Zum Präventivgewahrsam:** Die Änderungen verstoßen zum Teil gegen die **EMRK** und den Grundsatz der **Verhältnismäßigkeit**. Die Möglichkeit einer **bis zu zwei Monaten andauernden Freiheitsentziehung** im Rahmen des Polizeirechts **ist entschieden abzulehnen**.

Büro Kiel

Prof. Dr. Michael Gubitz
Dr. Martin Schaar
Dr. Wolf Molkentin
Dr. Momme Buchholz
Niklas Weber

Rechtsanwälte
Fachanwälte für Strafrecht

Dr. Stefan Bauhofer
Malte Buttenschön

Rechtsanwälte

Louisa Schultheis
Rechtsanwältin

Dänische Straße 15
24103 Kiel

tel 0431.5459770
fax 0431.5459772

kiel@gubitz-partner.de
www.gubitz-partner.de

Büro Hamburg

Dr. Ole-Steffen Lucke
Rechtsanwalt
Fachanwalt für Strafrecht

Dr. André Neumann
Rechtsanwalt
Fachanwalt für Strafrecht
Fachanwalt für Steuerrecht

Anna Kell
Rechtsanwältin

Prof. Dr. Gereon Wolters
Kooperationspartner

Stadthausbrücke 4
(Palaishof)
20355 Hamburg

tel 040.35718212
fax 040.35004199

hamburg@gubitz-partner.de
www.gubitz-partner.de

- **Elektronische Aufenthaltsüberwachung:** Die Änderungen beeinträchtigen den Hauptzweck der Maßnahmen – den **Schutz Betroffener häuslicher Gewalt** – und verstoßen teilweise gegen den Grundsatz der **hypothetischen Datenneuerhebung**.
- **Videoüberwachung:** Die Änderungen sind zur Verbesserung von **Gefahrenabwehr ungeeignet** und verstoßen aufgrund ihrer **Eingriffsintensität** gegen den Grundsatz der **Verhältnismäßigkeit**.
- **Biometrische Fernidentifizierung:** Sämtliche vorgesehenen Varianten der biometrischen Fernidentifizierung sind **europarechtswidrig**. Gegen einzelne Aspekte bestehen zudem **verfassungsrechtliche Bedenken**.

I. Ausdehnung des Präventivgewahrsams im Hinblick auf seine Dauer und seinen Anwendungsbereich

Durch den Gesetzesentwurf soll sowohl eine zeitliche Höchstdauer des Präventivgewahrsams geregelt werden als auch ein Auffangtatbestand für Fälle geschaffen werden, in denen eine Rechtsgutsverletzung noch nicht unmittelbar bevorsteht.

Während die Schaffung eines **Auffangtatbestands** im Rahmen des Präventivgewahrsams **vollständig abzulehnen** ist, ist die Normierung der Höchstdauer des Präventivgewahrsams grundsätzlich zu begrüßen, aber mit zwei Monaten (viel) zu hoch angesetzt. Auch bei den geschaffenen Auslegungshilfen und der Ausweitung der Möglichkeiten der audiovisuellen Überwachung im Gewahrsamsraum bezieht sich die Kritik lediglich auf **Teilaspekte** des Gesetzesentwurfs.

1. Ausdehnung des Anwendungsbereichs durch Schaffung eines Auffangtatbestands

§ 204 Abs. 1 Nr. 3 des Entwurfs ermöglicht es, eine Person in Gewahrsam zu nehmen, wenn dies unerlässlich ist zur Abwehr einer Gefahr für Leib, Leben oder Freiheit oder die sexuelle

Selbstbestimmung einer Person. Der **Auffangtatbestand**, der durch § 204 Abs. 1 Nr. 3 des Entwurfs geschaffen werden soll, verzichtet bewusst auf das Erfordernis einer *gegenwärtigen* Gefahr. Da es sich bei dem Präventivgewahrsam um einen besonders schwerwiegenden Eingriff in die Rechte der betroffenen Person handelt, ergeben sich aber erhebliche Bedenken hinsichtlich der Verhältnismäßigkeit der Maßnahme unterhalb der Eingriffsschwelle der gegenwärtigen Gefahr. Der Präventivgewahrsam lässt sich aufgrund seiner Eingriffsintensität nur dann mit dem Grundsatz der Verhältnismäßigkeit in Einklang bringen, wenn er zu einer situationsspezifisch kurzfristig erforderlichen Verhinderung einer **unmittelbar bevorstehenden Rechtsgutsverletzung** unumgänglich ist.¹

2. Verstoß gegen EMRK

Die vorgesehenen Absenkungen der Voraussetzungen für den Präventivgewahrsam kollidieren mit **Art. 5 Abs. 1 EMRK**.

a) Entgegen EGMR kein Erfordernis einer erhöhten Wahrscheinlichkeit

Art. 5 Abs. 1 EMRK enthält einen abschließenden Katalog von Fällen, in denen einer Person die Freiheit entzogen werden darf. Der Präventivgewahrsam wird nicht ausdrücklich genannt. Es kommt allenfalls² eine Rechtfertigung aus Art. 5 Abs. 1 lit. c EMRK mit Art. 5 Abs. 1 EMRK in Betracht.

¹ Hierzu auch *Löffelmann* GSZ 2021, 164, 166. Der Umstand, dass unterhalb der Eingriffsschwelle einer gegenwärtigen Gefahr eine Person nicht zum Zwecke der Gefahrenabwehr in Gewahrsam genommen werden kann, stellt keine schließungsbedürftige Lücke dar. Gerade bei so eingriffsintensiven Maßnahmen kann die Begrenzung ihres Anwendungsbereichs die notwendige Konsequenz einer Abwägung mit den grundrechtlich geschützten Gegeninteressen sein. Nicht jede Lücke im Rahmen polizeilicher Handlungsermächtigungen bedarf daher der Schließung. Dies gilt insbesondere im Hinblick auf das in der Entwurfsbegründung angeführte Beispiel (Drucks. 20/4284 S. 2): Der genannte Messerangriff in der Kieler Innenstadt hätte auch nicht durch die vorgeschlagene Erweiterung des Anwendungsbereichs des Präventivgewahrsams unterbunden werden können, da der Täter vor Begehung der Tat nicht polizeilich auffällig geworden ist. Es gab somit auch keine Anhaltspunkte, die die Annahme gerechtfertigt hätten, dass es unerlässlich sei, ihn zur Abwehr einer Gefahr für Leib oder Leben in Gewahrsam zu nehmen.

² Art. 5 Abs. 1 lit. b EMRK soll hier nur in einer Fußnote erwähnt werden. Er erlaubt die Freiheitsentziehung wegen Nichtbefolgung einer rechtmäßigen gerichtlichen Anordnung oder zur Erzwingung der

Art. 5 Abs. 1 lit. c EMRK erlaubt die Freiheitsentziehung unter anderem, wenn ein begründeter Anlass zu der Annahme besteht, dass die Freiheitsentziehung notwendig ist, um die betroffene Person an der Begehung einer Straftat zu hindern. Nach der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte, muss „*die Straftat [...] insbesondere nach Ort und Zeit sowie ihren Opfern bestimmt sein*“.³ Darüber hinaus ist es erforderlich, dass „*der Betroffene sehr wahrscheinlich die konkrete und bestimmte Straftat begangen hätte, wenn deren Begehung nicht durch die Haft verhindert worden wäre*“.⁴

+ Diesen Anforderungen wird der Auffangtatbestand nicht gerecht. Neben dem Erfordernis einer hinreichenden Konkretisierung der Straftat wird nach der Rechtsprechung des EGMR zusätzlich vorausgesetzt, dass die Begehung der Straftat durch den Betroffenen „*sehr wahrscheinlich*“ gewesen sein muss. Dieses Erfordernis geht über die im Gesetzesentwurf vorgesehene Wahrscheinlichkeitsschwelle hinaus. Im Entwurf soll eine *konkrete* Gefahr für die näher bezeichneten Rechtsgüter ausreichen. Im Rahmen einer konkreten Gefahr genügt die *hinreichende Wahrscheinlichkeit*. Zum Bestimmen des Vorliegens der hinreichenden Wahrscheinlichkeit ist nach dem Bundesverwaltungsgericht eine Abwägung vorzunehmen: Je schwerer der zu befürchtende Schaden wiegt und je höherwertiger das betroffene Rechtsgut ist, desto geringer kann die Wahrscheinlichkeit des Schadenseintritts sein.⁵

+

Weil im Rahmen von § 204 Abs. 1 Nr. 3 des Entwurfs nur Gefahren für besonders gewichtige Rechtsgüter erfasst sind, reicht schon

Erfüllung einer gesetzlichen Verpflichtung. In einer Entscheidung aus dem Oktober 2018 hat die große Kammer des Europäischen Gerichtshofs für Menschenrechte entschieden, dass die Pflicht keine Straftaten zu begehen nur dann den Anforderungen des Art. 5 Abs. 1 lit. b EMRK genügt, „wenn Ort und Zeit der unmittelbar bevorstehenden Straftat und ihre möglichen Opfer ausreichend präzisiert sind, der Betroffene unterrichtet worden ist, welche bestimmte Tat er unterlassen muss, und nicht bereit ist, das zu tun“. Sie genügt den Anforderungen nicht, „solange keine bestimmten Maßnahmen angeordnet worden sind, denen der Betroffene nicht nachgekommen ist“. Der Auffangtatbestand, der durch den Entwurf geschaffen werden soll, verzichtet zum einen bewusst auf das Erfordernis einer gegenwärtigen Gefahr und somit auch auf das Erfordernis des unmittelbaren Bestehens einer Rechtsgutsschädigung oder einer Straftat. Zum anderen enthält er nicht das Erfordernis, dass gegenüber der betroffenen Person im Vorfeld eine bestimmte Maßnahme angeordnet werden musste, der der Betroffene nicht Folge geleistet haben darf.

³EGMR NVwZ 2019, 135, 137 Rdnr. 89 mit weit. Nachw.

⁴EGMR NVwZ 2019, 135, 137 f. Rdnr. 91.

⁵BVerwG WKRS 1991, 12406 Rdnr. 13.

eine geringe tatsächliche Wahrscheinlichkeit für die Annahme der Voraussetzungen einer konkreten Gefahr. Damit werden aber die Anforderungen des EGMR unterlaufen.

Die Anforderungen, die § 204 Abs. 1 Nr. 3 des Entwurfs an die Anordnung des Präventivgewahrsams stellt, bleiben somit hinter den Mindestanforderungen des Art. 5 Abs. 1 EMRK zurück, so dass der Auffangtatbestand in seiner aktuell vorgesehenen Ausgestaltung als konventionswidrig anzusehen ist.

b) Fehlende Begrenzung der Ingewahrsamnahme auf Störer*innen

Ein Verstoß gegen die EMRK könnte sich auch aus dem Umstand ergeben, dass § 204 Abs. 1 Nr. 3 des Entwurfs den Kreis der möglichen Betroffenen nicht auf Störer*innen begrenzt. Zumindest abstrakt wäre über § 220 Abs. 1 LVwG somit auch die Ingewahrsamnahme der Person, deren Rechtsgüter gefährdet sind, möglich. Eine solche Praxis würde eindeutig gegen Art. 5 EMRK verstoßen.

3. Explizite Normierung der Höchstdauer

Auch wenn die explizite Normierung der **Höchstdauer** zu begrüßen ist, darf nicht verkannt werden, dass die gewählte Maximaldauer nicht zu einer Verkürzung, sondern zu einer Verlängerung der in der Praxis vorkommenden Fälle des Präventivgewahrsams führen wird. Bisher wurden in Schleswig-Holstein Personen faktisch nur für kurze Zeit in Gewahrsam genommen.⁶ Wenn es lediglich um die Schaffung von Rechtsklarheit gehen würde, wäre es somit naheliegend, eine kürzere Höchstdauer – von wenigen Tagen oder bis zu zwei Wochen – im Entwurf aufzunehmen. Stattdessen wurde sich – wie auch schon bei der Schaffung des Auffangtatbestands – an der bayrischen Rechtslage orientiert. Die in Bayern zulässige Gesamtdauer von zwei Monaten liegt **deutlich über der zulässigen Höchstdauer des Präventivgewahrsams**

⁶ <https://www.lto.de/recht/meinung/m/meinung-entscheidung-bayerischer-verfassungsgerichtshof-polizeiaufgabengesetz-bayern>.

sämtlicher anderer Bundesländer. Die Orientierung an den bayrischen Maßstäben ist gerade in Anbetracht der Eingriffsintensität und des Umstandes, dass auch der Präventivgewahrsam Teil des Normkontrollverfahrens in Sachen „Bayerisches Polizeiaufgabengesetz“ ist, welches aktuell vor dem Bundesverfassungsgericht verhandelt wird, kritisch zu betrachten. Ein Urteil steht noch aus.

Eine Höchstgrenze von insgesamt zwei Monaten könnte auch mit dem Charakter des polizeilichen Präventivgewahrsams *„als Maßnahme der kurzfristigen Krisenbewältigung“*⁷ unvereinbar sein.

Der Präventivgewahrsam lässt sich aufgrund seiner Eingriffsintensität nur dann mit dem Grundsatz der Verhältnismäßigkeit in Einklang bringen, wenn er zu einer situationsspezifisch kurzfristig erforderlichen Verhinderung einer unmittelbar bevorstehenden Rechtsgutsverletzung unumgänglich ist.⁸ Ab welcher Dauer die Grenze einer solchen Kurzfristigkeit überschritten ist, wurde noch nicht abschließend durch die Rechtsprechung geklärt. Aus einem Urteil des Bundesverfassungsgerichts aus dem Februar 2004 lässt sich jedoch eine gewisse Tendenz ableiten. Hierin heißt es, dass *„der Staat auf konkrete Gefahrensituationen lediglich mit den situationsbezogenen Instrumenten des Polizeirechts reagieren [darf], zu denen auch der bis zu 14-tägige landesrechtliche Polizeigewahrsam gehören dürfte. Dagegen wäre die längerfristige Verwahrung eines psychisch gesunden und strafrechtlich nicht oder nur unerheblich vorbelasteten Bürgers zum Zweck der Abwehr einer von ihm ausgehenden Gefahr der Begehung von Straftaten mit dem Grundgesetz nicht vereinbar“*.⁹

Hieraus ergibt sich zwar nicht, dass das Bundesverfassungsgericht 14 Tage als absolute Höchstgrenze des Präventivgewahrsams ansieht; dennoch folgt aus der expliziten Nennung der nach dem Polizeirecht zulässigen Höchstdauer im Kontrast zur längerfristigen Verwahrung, dass zumindest bei einer deutlichen Überschreitung der Zwei-Wochen-Grenze die Stufe der längerfristigen Verwahrung erreicht wird. Ab diesem Zeitpunkt **verliert der**

⁷ Lisken/Denninger/Bäcker PolR-HdB/Bäcker Kap. 4 Rdnr. 514.

⁸ Hierzu auch Löffelmann GSZ 2021, 164, 166.

⁹ BVerfG Urteil v. 10. Februar 2004 – 2 BVR 1588/02 – Rdnr. 111.

Präventivgewahrsam seinen Charakter als situationsspezifisch kurzfristiges Schutzinstrument.

Zumindest die Gesamtdauer des Präventivgewahrsams von bis zu zwei Monaten wird dementsprechend in Anbetracht des zeitlich ansteigenden Eingriffsgewichts von Freiheitsentziehungen stets als unverhältnismäßig einzuordnen sein.¹⁰

Anders als im Polizeirecht einiger anderer Bundesländer findet sich im Rahmen der im Entwurf vorgesehenen Höchstdauer auch keine Abgrenzung zwischen Schutzgewahrsam und Unterbindungsgewahrsam. Da diese beiden Gewahrsamsformen grundlegend unterschiedlicher Natur sind, wäre auch eine unterschiedliche Höchstgrenze angezeigt.¹¹

4. Videoüberwachung im Gewahrsamsraum

Durch § 205 Abs. 6 des Entwurfs soll die im geltenden Recht in § 204 Abs. 4 S. 2 LVwG geregelte Möglichkeit der **Beobachtung der in Gewahrsam genommenen Person** durch Bildübertragung ausgeweitet werden.

Während eine solche Übertragung aktuell nur zum **Schutz der betroffenen Person** möglich ist, soll sie künftig **auch zum Schutz im Gewahrsamsraum anwesender Polizeivollzugsbeamt*innen** möglich sein. Es sollen zudem **Bild- und Tonaufzeichnung** angefertigt werden können.

In der Entwurfsbegründung heißt es hierzu, dass „*die Bundesstelle zur Verhütung von Folter [...] in ihrem Jahresbericht 2016 zu dem Schluss [kommt], dass [sich] der Einsatz von Video- und Tonüberwachung in Gewahrsamsräumen [...] positiv zum Schutz aller involvierten Personen auswirkt*“.¹² (Drucks. 20/4284 S. 76). Eine Ausweitung des Schutzes der in Gewahrsam genommen Person wird durch den Entwurf jedoch nicht erreicht. Bei der Anwesenheit von Polizeivollzugsbeamt*innen soll eine Bildübertragung

¹⁰ Hierzu auch Lisken/Denninger/Bäcker PolR-HdB/Bäcker Kap. 4 Rdnr. 517.

¹¹ Hierzu auch BeckOK PolR Bayern/Grünwald/Hahn Art. 20 PAG Rdnr. 17. Der Schutzgewahrsam dient dem Schutz *der* in Gewahrsam genommenen Person, während der Unterbindungsgewahrsam dem Schutz *vor der* in Gewahrsam genommenen Person dient.

¹² Drucks. 20/4284 S. 76.

nämlich nur zulässig sein, soweit sie zum Schutz der Polizeivollzugsbeamt*innen oder der in Gewahrsam befindlichen Person unerlässlich ist. Sie soll dementsprechend **nicht verpflichtend** sein. Die Frage der Unerlässlichkeit wird jedoch bei lebensnaher Betrachtung im Einzelfall durch die Vollzugsbeamt*innen selbst beantwortet werden. Es ist daher davon auszugehen, dass **Übergriffe durch Vollzugsbeamt*innen** auf die in Gewahrsam befindliche Person durch die Videoüberwachung gerade nicht aufgezeichnet werden.

Die Schutzfunktion, von der in der Entwurfsbegründung die Rede ist, kann die Videoüberwachung somit nur dann erfüllen, wenn sie stets verpflichtend wäre. Die aktuelle Fassung schützt nicht alle „Involvierten“, sondern allenfalls Polizeivollzugsbeamt*innen.

II. Elektronische Aufenthaltsüberwachung

Der Gesetzesentwurf schlägt eine sowohl redaktionelle als auch teilweise inhaltliche Umgestaltung der Regelungen zur elektronischen Aufenthaltsüberwachung vor. Während die redaktionellen Änderungen unbeanstandet bleiben können, sind zwei inhaltliche Teilaspekte der Novellierung kritisch zu würdigen.

1. Ausweitung der Anwendungsfälle der elektronischen Aufenthaltsüberwachung durch den Verzicht auf die individuelle Bestimmbarkeit der gefährdeten Person

Während § 201c LVWG des geltenden Rechts die elektronische Aufenthaltsüberwachung zum Schutz einer bestimmten gefährdeten Person zulässt, verzichtet der Gesetzesentwurf auf die **individuelle Bestimmbarkeit der gefährdeten Person**. Hierdurch **entfernt** sich die Ermächtigungsgrundlage von ihrem ursprünglichen Hauptzweck, dem **Schutz vor häuslicher Gewalt und Stalking-Fällen**.

Schon jetzt: Anwendungsdefizit

Zu diesem eigentlichen Hauptzweck wird bereits aktuell äußerst selten von der Möglichkeit der elektronischen Aufenthaltsüberwachung Gebrauch gemacht. Bei einer Erhebung für den Stichtag

des 30. Juni 2026¹³ wurden 147 Personen festgestellt, die mit einer elektronischen Fußfessel überwacht wurden. 128 davon wurden im Rahmen der **Führungsaufsicht** überwacht und eine auf Grundlage des Aufenthaltsgesetz. In sämtlichen Bundesländern zusammengekommen wurden dementsprechend nur 18 Personen auf Grundlage des Polizeirechts überwacht. Hierzu gehörten nicht nur Personen, die zum Schutz vor häuslicher Gewalt überwacht wurden, sondern ebenso Personen, von denen eine terroristische Gefahr ausging.

Bevor nun die elektronische Aufenthaltsüberwachung auf weitere Gefahrensituationen ausgeweitet wird, ist eine Überprüfung des Anwendungsdefizits zu fordern. Die rechtlichen Grundlagen für einen Grundrechtseingriff, der bereits jetzt an der praktischen Umsetzung scheitert, dürfen nicht noch ausgeweitet werden.

Sollte die geringe Fallzahl überwachter Personen zumindest anteilig auf geringen personellen oder materiellen Kapazitäten beruhen, würde die Ausweitung des Anwendungsbereichs der elektronischen Aufenthaltsüberwachung überdies mit der Gefahr einhergehen, dass die durch häusliche Gewalt und Stalking gefährdeten Personen noch seltener durch die elektronische Aufenthaltsüberwachung geschützt werden. Sie konkurrieren dann mit den erweiterten Fällen, in denen die elektronische Aufenthaltsüberwachung möglich wird.¹⁴

2. Weiterverarbeitung der durch die Überwachung erlangten Daten zum Zweck der Vorbereitung und Durchführung der Abschiebung

Die **Weiterverarbeitung** der durch die Überwachung erlangten Daten **zum Zweck der Vorbereitung und Durchführung der Abschiebung**, welche durch § 201b Abs. 6 S. 1 Nr. 4 des Entwurfs ermöglicht werden soll, ist strikt abzulehnen.

¹³ <https://www.lto.de/recht/nachrichten/n/elektronische-fussfessel-147-personen-ueberwacht>.

¹⁴ Darüber hinaus ist festzuhalten, dass der in der Entwurfsbegründung genannte Messerangriff in der Kieler Innenstadt auch durch die Ausweitung des Anwendungsbereichs der elektronischen Aufenthaltsüberwachung nicht hätte verhindert werden können, da der Täter vor der Tatbegehung nicht auffällig geworden ist (ein Kollege des Unterzeichners ist mit dem Fall befasst gewesen).

a) Widerspruch zu den Wertungen des Aufenthaltsgesetzes

Durch den Entwurf sollen die mithilfe der elektronischen Aufenthaltsüberwachung erlangten Daten schon beim Verdacht einer Straftat im Sinne des § 54 Abs. 1 Nr. 1a AufenthG oder wenn Anhaltspunkte für das Vorliegen eines Ausweisungsinteresses im Sinne von § 54 Abs. 1 Nr. 2-5 AufenthG vorliegen, zur Vorbereitung und Durchführung der Abschiebung der überwachten Person weiterverarbeitet werden können. Dies ist mit der **Wertung der primären Rechtsnorm des Aufenthaltsgesetzes nicht vereinbar**:

§ 54 Abs. 1 AufenthG führt Fälle auf, bei denen das Ausweisungsinteresse besonders schwer wiegt. Zu beachten ist hierbei jedoch, dass § 54 Abs. 1 Nr. 1a AufenthG von einem besonders schwerwiegenden Ausweisungsinteresse **erst bei einer rechtskräftigen Verurteilung zu einer Freiheitsstrafe von mindestens einem Jahr** aufgrund einer oder mehrerer der genannten Straftaten ausgeht. Der Verdacht allein reicht **gerade nicht** aus.

Auch kann ein schwerwiegendes Ausweisungsinteresse im Sinne des § 54 Abs. 2 AufenthG nicht allein auf den Verdacht einer Straftat gestützt werden. Vergleichbares gilt für die weiteren von § 201b Abs. 6 S. 1 Nr. 4 des Entwurfs erfassten Nummern des § 54 Abs. 1 AufenthG. Auch hier reicht das Vorliegen (nur) tatsächlicher Anhaltspunkte für das Bestehen eines besonders schwerwiegenden Ausweisungsinteresses nicht.

Die Neuregelung würde entgegen der Wertung des Aufenthaltsgesetzes eine Weiterverarbeitung der Daten der elektronischen Aufenthaltsüberwachung somit auch möglich werden lassen, wenn noch kein schweres oder besonders schweres Ausweisungsinteresse vorliegt.¹⁵

¹⁵ Selbst die aufenthaltsrechtliche Anordnung, sich mindestens einmal wöchentlich bei der polizeilichen Dienststelle zu melden, erfordert das Vorliegen eines besonders schweren Ausweisungsinteresses im Sinne von § 54 Abs. 1 Nr. 2-5 AufenthG (§ 56 Abs. 1 S. 1 AufenthG). Die Voraussetzungen einer solchen Anordnung liegen somit erheblich höher als die der Weiterverarbeitung der im Wege der elektronischen Aufenthaltsüberwachung erlangten Daten zum Zwecke der Vorbereitung und Durchführung einer Abschiebung der überwachten Person, die der Entwurf in § 201b Abs. 6 Nr. 4 vorsieht. Dies erscheint gerade in Anbetracht dessen, dass die Weiterverarbeitung einen eigenen neuen Eingriff in das Grundrecht der betroffenen Person auf informationelle Selbstbestimmung darstellt, höchst problematisch.

b) Verstoß gegen den Grundsatz der hypothetischen Datenneuerhebung

Es ist davon auszugehen, dass die in § 201b Abs. 6 Nr. 4 des Entwurfs enthaltene Möglichkeit der Weiterverarbeitung der Aufenthaltsdaten zum Zwecke der Vorbereitung und Durchführung der Abschiebung, dem vom Bundesverfassungsgericht geprägten **Grundsatz der hypothetischen Datenneuerhebung** nicht genügt.

Nach diesem Grundsatz soll eine Weiterverarbeitung von Daten aus eingriffsintensiven Überwachungsmaßnahmen, zu denen die durch die elektronische Aufenthaltsüberwachung erlangten Daten zählen, zu einem anderen als ihrem Ursprungszweck (Zweckänderung) möglich sein, wenn *„die entsprechenden Daten nach verfassungsrechtlichen Maßstäben neu auch für den geänderten Zweck mit vergleichbar schwerwiegenden Mitteln erhoben werden dürften“*.¹⁶ Hieran fehlt es aber offensichtlich, da selbst § 56a AufenthG eine elektronische Aufenthaltsüberwachung allenfalls zum Zwecke der Abwehr einer erheblichen Gefahr für die innere Sicherheit oder für Leib und Leben Dritte und nicht zur Vorbereitung oder Durchführung der Abschiebung der Person ermöglicht. § 56a AufenthG enthält auch keine Möglichkeit der Weiterverarbeitung der erlangten Aufenthaltsdaten zu diesem Zweck.

Darüber hinaus ist eine Zweckänderung nur dann zulässig, wenn *„die neue Nutzung der Daten dem Schutz von Rechtsgütern oder der Aufdeckung von Straftaten eines solchen Gewichts dient, die verfassungsrechtlich ihre Neuerhebung mit vergleichbar schwerwiegenden Mitteln rechtfertigen könnten“*.¹⁷ Auch dieser Anforderung wird der Entwurf offensichtlich nicht gerecht, da weder die Vorbereitung noch die Durchführung der Abschiebung unmittelbar dem Schutz von Rechtsgütern dient. Dies wird besonders dadurch deutlich, dass eine Weiterverarbeitung auf dem Verdacht der Begehung einer Straftat in der Vergangenheit beruhen können soll. Hierbei handelt es sich um eine retrospektive Erwägung, die für den zukünftigen Schutz von Rechtsgütern zunächst einmal

¹⁶ BVerfG NJW 2016, 1781, 1801 Rdnr. 287 mit weit. Nachw.

¹⁷ BVerfG NJW 2016, 1781, 1802 Rdnr. 288.

ohne Belang ist. Die Abschiebung der betroffenen Person ist zudem für die Aufklärung der Straftat nicht zuträglich, sondern hinderlich. Der Zweck der Weiternutzung – die Vorbereitung und Durchführung der Abschiebung – ist somit zum Schutz von Rechtsgütern oder der Aufdeckung von Straftaten **ungeeignet** und kann daher auch aus diesen Gesichtspunkten **verfassungsrechtlich nicht gerechtfertigt** sein.

III. Ausweitung der Videoüberwachung

1. Absenkung der Anforderungen an die Anfertigung von Bild und Tonaufnahmen

§ 184 Abs. 3: **Erweiterung** auf **gefährdete Orte**, also Verkehrs- oder Versorgungsanlagen oder -einrichtungen, öffentliche Verkehrsmittel, Amtsgebäude und das jeweilige Umfeld dieser Orte.

Die Anfertigung von **Bildaufnahmen** und deren Speicherung anstelle bloßer **Beobachtung** an allen **sonstigen**, der Allgemeinheit zugänglichen Orten soll möglich werden, wenn dies **im Einzelfall zur Abwehr einer Gefahr für die öffentliche Sicherheit** erforderlich ist.

§ 184 Abs. 3 des Entwurfs weitet zudem die Möglichkeit der **Anfertigung von Tonaufnahmen** auf sämtliche Fälle aus, in denen Bildaufnahmen angefertigt werden dürfen.

Die vorgesehenen Neuerungen sind abzulehnen.

Die Annahme der Entwurfsbegründung, diese Erweiterung sei zur flexiblen Gefahrenabwehr und zum Schutz besonders schützenswerter Einrichtungen erforderlich,¹⁸ vermag nicht zu überzeugen.

Die **Speicherung von Aufnahmen** stellt im Verhältnis zur reinen Übertragung einen weiteren **zusätzlichen Eingriff** in das Recht auf informationelle Selbstbestimmung dar, welcher auf der Möglichkeit einer späteren Durchsicht der Aufnahmen beruht.¹⁹ Dieser zusätzliche Eingriff könnte allenfalls gerechtfertigt sein, wenn die Anfertigung von Aufnahmen aus einer

¹⁸ Drucks. 20/4284 S. 40.

¹⁹ BVerfG Beschluss v. 17. Februar 2009 – 1 BvR 2492/08 – Rdnr. 129 ff.

Gefahrenabwehrperspektive **signifikante Vorteile** gegenüber der reinen Bildübertragung aufweisen würde.

Eine Begründung hierfür bleiben die Entwurfsverfasser schuldig.

Denkbar sind langandauernde oder sich wiederholende Gefährdungslagen für die geschützten Einrichtungen – jedoch dürften diese Konstellationen besondere Ausnahmen darstellen. Ohne weiteres können solche aber nicht zur Grundlage weitreichender Grundrechtseingriffe auch Unbeteiligter (dazu sogleich) gemacht werden, zudem werden in diesen Fällen regelmäßig andere Mittel zu Gebote stehen.

a) Große Zahl Unbeteiligter betroffen

Zudem ist zu befürchten, dass von der Ausweitung der Videoüberwachung und der Anfertigung von Bild und Tonaufnahmen ein sehr großer Kreis von Personen betroffen sein wird, die durch ihr Verhalten keinerlei Anlass für die Maßnahme gegeben haben.

Als unmittelbares Umfeld gefährdeter Orte wird der Bereich angesehen, von dem ein Angriff auf den gefährdeten Ort möglich ist. Hierunter sollen Orte in einem Radius von bis zu zwei Kilometer fallen können.²⁰ Damit könnten beispielsweise große Teile des Kieker Stadtgebiets mittels der Anfertigung von Aufnahmen zu überwachen sein.

In Anbetracht des auf wenige Einzelfälle beschränkten Mehrwerts, den die Anfertigung von Aufnahmen gegenüber der Bildübertragung erbringen könnte, ist ein derart weit gefasster Anwendungsbereich als unverhältnismäßig abzulehnen.

b) Verstärkung der Einschüchterungswirkung durch Tonaufzeichnungen

Dies gilt umso mehr für die vorgesehene Möglichkeit der Erstellung von **Tonaufzeichnungen**.

²⁰ Lisken/Denninger/Bäcker PolR-HdB/Barczak Kap. 4 Rdnr. 278 mit weit. Nachw.

Die bei jeder Anfertigung von Aufnahmen bestehende Gefahr der Einschüchterungswirkung²¹ steigt durch die Erstellung von Tonaufnahmen noch einmal erheblich. Menschen, denen bewusst ist, dass sie nicht nur durch Kameras beobachtet werden, sondern auch Tonaufnahmen noch nachträglich ausgewertet werden, werden ihr Verhalten anpassen. Es macht einen erheblichen Unterschied im Verhalten aus, ob sich jemand unbeobachtet oder überwacht und abgehört fühlt. Es wird dann nämlich nicht nur auf verbotene Handlungen, sondern auch auf erlaubte Handlungen verzichtet.²² Es kommt somit zu einem Effekt der Selbstzensur bezogen auf Handlungen und Äußerungen im öffentlichen Raum.

Das ist nicht zu rechtfertigen.

2. Automatische Erkennung von Bewegungsmustern

Durch § 184 Abs. 5 des Gesetzesentwurfs soll zudem die Grundlage der **automatisierten Datenverarbeitung zur Erkennung bestimmter Bewegungsmuster** geschaffen werden, die auf Handlungen hindeuten, mit welchen Leben, Leib, Freiheit oder die sexuelle Selbstbestimmung einer Person beeinträchtigt werden. Die erkannten Muster sind durch Polizeibeamt*innen zu prüfen. Diese haben dann die Möglichkeit, die jeweilige Person zu kennzeichnen, wodurch diese dann automatisiert über mehrere Kamerabilder nachverfolgt werden kann.

In der Entwurfsbegründung heißt es dazu, dass die Software in der Lage sein soll, „*Video- und Audiodateien automatisiert zu erfassen und zu analysieren*“, um etwa Tumulte, Schlagbewegungen oder bestimmte Gegenstände zu erkennen.²³

Die Analyse von *Audiodateien* ist jedoch zur Erkennung von *Bewegungsmustern* offensichtlich **ungeeignet**.

Auch das *Erkennen* von Gegenständen unterfällt nicht der vorgesehenen Ermächtigungsgrundlage. Allenfalls ihre *Verwendung* kann unter den Begriff des Bewegungsmusters fallen.

²¹ BVerfG Beschluss v. 17. Februar 2009 – 1 BvR 2492/08 – Rdnr. 131.

²² Hierzu BVerfG Beschluss v. 17. Februar 2009 – 1 BvR 2492/08 – Rdnr. 131.

²³ Drucks. 20/4284 S. 34.

Polizist*innen sollten außerdem in der Lage sein, Schlagbewegungen und Tumulte auch ohne den Einsatz von besonderen (KI-) Programmen zu erkennen.

In den genannten Beispielen – der Erkennung von Schlagbewegungen und Tumulten – wird die jeweilige Gefahr, die erkannt wird, zudem zumeist bereits beendet sein, bevor durch Folgemaßnahmen eingegriffen werden könnte. Zur Gefahrenabwehr ist die im Entwurf vorgesehene automatisierte Datenverarbeitung somit ungeeignet.

Darüber hinaus sind sogenannte Verhaltensscanner extrem **fehleranfällig**. Im Rahmen der Erprobung entsprechender Verhaltensscanner in Hamburg konnte durch das Forschungsprojekt „Lokale Öffentlichkeit und soziale Konflikte um KI-gestützte Sicherheitstechnologie“ festgestellt werden, dass 99 Prozent der markierten Bewegungsmuster fälschlicherweise gekennzeichnet wurden.²⁴

Gerade in Anbetracht dessen, dass die automatisierte Verhaltensanalyse einen eigenen, über die Videoüberwachung hinausgehenden Eingriff in das Recht auf informationelle Selbstbestimmung darstellt, ist eine derart ungeeignete Maßnahme als unverhältnismäßig anzusehen.

Insgesamt ist daher auf die vorgeschlagenen Änderungen des § 184 LVwG zu verzichten.

IV. Einführung der biometrischen Fernidentifizierung

Durch den Gesetzesentwurf soll ein rechtlicher Rahmen für die softwaregestützte biometrische Fernidentifizierung geschaffen werden. Hierbei werden biometrische Referenzdaten von einer Person gewonnen, welche mit Vergleichsdaten auf Übereinstimmungen überprüft werden, um eine Person zu identifizieren. Der Gesetzesentwurf unterscheidet drei verschiedene Formen der biometrischen Fernidentifizierung.

²⁴ <https://netzpolitik.org/2026/verhaltensscanner-in-hamburg-die-polizei-wird-zum-datenlieferant/>.

1. § 195 Abs. 2 des Entwurfs: Die Identifizierung erfolgt nachträglich anhand von Referenz- und Vergleichsdaten, **die bereits rechtmäßig in Polizeidatenbanken gespeichert** sind.
2. § 195b des Entwurfs: Die Identifizierung erfolgt nachträglich durch den Abgleich der Referenzdaten mit Vergleichsdaten, die **aus im Internet öffentlich zugänglichen Daten** gewonnen werden.
3. § 184b des Entwurfs: Die Identifizierung erfolgt in Echtzeit durch den Abgleich mit Daten die durch eine automatisierte Anwendung von Personen erlangt werden, die **durch Kameras und Mikrofone im öffentlich zugänglichen Raum aufgenommen** werden.

Sämtliche drei Formen der biometrischen Fernidentifizierung sind abzulehnen. Keine der Varianten ist in ihrer geltenden Fassung mit den europarechtlichen Vorgaben vereinbar. Teilweise bestehen zudem verfassungsrechtliche Bedenken.

Selbst bei einer europarechtskonformen Ausgestaltung ist die Einführung der biometrischen Fernidentifizierung aufgrund der **diskriminierenden Wirkung** sogenannter „false positives“ abzulehnen. „False positives“ sind fälschlich angezeigte Treffer, also hier die Markierung zweier unterschiedlicher Menschen als dieselbe Person. Eine Studie des „National Institute of Standards and Technology“²⁵ kam zu dem Ergebnis, dass die Anzahl von „false positives“ bei dem Abgleich biometrische Gesichtsdaten von Personen, die nicht einem mittel- bis nordeuropäischen Phänotypen („Caucasian“) entsprechen, bis zu 100fach erhöht ist. Die Gefahr durch den Einsatz von einer biometrischen Fernidentifizierung fälschlicherweise als Störer*in identifiziert zu werden und anlasslos von polizeilichen Nachfolmaßnahmen betroffen zu sein, ist somit für migrantisierte Personen um ein Vielfaches höher.

Dieser Diskriminierungseffekt wird auch nicht dadurch beseitigt, dass das Ergebnis der Fernidentifizierung noch durch zwei

²⁵ Abrufbar über: <https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software>.

Beschäftigte der Polizei zu überprüfen ist (§ 184c Abs. 1 S. 2 und § 195c Abs. 1 S. 2 des Entwurfs). Die Erfahrung²⁶ zeigt, dass auch Polizeibeamten immer wieder Probleme bei dem Wiedererkennen von Gesichtern haben. Insbesondere bei Gesichtern, die nicht einem mittel- bis nordeuropäischen Phänotypen entsprechen, kommt es häufig zur Annahme von Übereinstimmungen, die in Wahrheit nicht gegeben sind.

Gerade durch die Häufung von „false positives“ erhöht sich die Gefahr, dass bereits aktuell durch polizeiliche Diskriminierung betroffene Personen häufiger zum Ziel ungerechtfertigter Polizeimaßnahmen werden. Ein falscher Treffer belegt die jeweilig falsch identifizierte Person in jedem Fall zumindest mit einem ungerechtfertigten Verdacht.

1. § 195 Abs. 2 des Entwurfs: Fernidentifizierung anhand vorhandener Polizeidaten

Da diese Vorschrift nur den Abgleich von Daten ermöglicht, die rechtmäßig in polizeilichen Datei- und Informationssystemen gespeichert sind, stellt der Entwurf an die biometrische Fernidentifizierung im Rahmen von § 195 Abs. 2 des Entwurfs die niedrigsten Anforderungen. Eine Fernidentifizierung soll unter anderem zur Feststellung der Identität einer Person, von der eine Gefahr für die öffentliche Sicherheit ausgeht, möglich sein, wenn der Abgleich zur Abwehr dieser Gefahr zwingend erforderlich ist.

Zu den rechtmäßig gespeicherten Daten nach dieser Vorschrift zählen jedoch auch sämtlich Bild- und Tonaufnahmen, die auf Grundlage des § 184 des Entwurfs erlangt worden sind. In Anbetracht der geringen Voraussetzungen, die die Anfertigung solcher Aufnahmen ermöglichen,²⁷ und dem Umstand, dass von ihnen eine große Anzahl an Nichtstörer*innen betroffen ist, ist die

²⁶ Auch in der Kanzlei des Unterzeichners gibt es aktuell einen Fall einer solchen Falschidentifizierung einer Person mit Migrationshintergrund, obwohl gegenüber der Täterbeschreibung optisch kaum Übereinstimmungen bestehen, die Personen unterschiedlich alt sind, aus unterschiedlichen Ländern kommen und an unterschiedlichen Orten wohnen. Hier kam es sogar zu einer Durchsuchung.

²⁷ Hierzu ausführlich unter III.

Weiterverarbeitung zum Zwecke der Fernidentifizierung kritisch zu bewerten.

a) Parallelen zur Rasterfahndung

Da die Daten, die durch die erweiterten Möglichkeiten der Videoüberwachung gewonnen wurden, grundsätzlich **verdachtslos** erlangt und mit einer großen Streubreite erhoben werden,²⁸ kann man bei ihrer Weiterverarbeitung zum Zwecke des Abgleichs²⁹ Parallelen zur Rasterfahndung ziehen. Dementsprechend wäre als Eingriffsvoraussetzung **eine konkrete Gefahr³⁰ für ein hochrangiges Rechtsgut zu fordern.**³¹

Die Vergleichbarkeit zwischen dem Abgleich der Daten, die im Wege von § 184 des Entwurfs zum Zwecke der Fernidentifizierung gewonnen wurden, und Fällen der Rasterfahndung kommt in der Entwurfsbegründung lediglich im Rahmen der Echtzeit-Fernidentifizierung zur Sprache. Hier heißt es:

„Nach der Rechtsprechung des BVerfG muss eine Rechtsgrundlage, welche die Gewinnung einer große[n] Datenmenge potenziell unbeteiligter Personen zum Zweck eines Abgleichs gestattet, der Abwehr konkreter Gefahren für hochrangige Rechtsgüter dienen [...]. Die zur Rasterfahndung formulierten Grundsätze gelten für eine Fernidentifizierung entsprechend, die sich Bild - und Tonaufnahmen oder -aufzeichnungen von Personen auf allgemein zugänglichen Flächen und in öffentlich zugänglichen Räumen als Datenquelle bedient. [...] Die biometrischen Echtzeit-Fernidentifizierung nach § 184b LVwG-Entwurf ist daher nur zulässig zur Abwehr einer konkreten Gefahr für

²⁸ Hierzu im Rahmen der Rasterfahndung: BVerfG Beschluss v. 4. April 2006 – 1 BVR 5108/02 – Rdnr. 116 ff.

²⁹ Hinsichtlich der Rasterfahndung: BVerfG Beschluss v. 4. April 2006 – 1 BVR 5108/02 – Rdnr. 73-79.

³⁰ BVerfG Beschluss v. 4. April 2006 – 1 BVR 5108/02 – Rdnr. 89, 133; BVerfG Urteil v. 20. April 2016 – 1 BvR 966/09 – Rdnr. 207.

³¹ BVerfG Beschluss v. 4. April 2006 – 1 BVR 5108/02 – Rdnr. 133; BVerfG Urteil v. 20. April 2016 – 1 BvR 966/09 – Rdnr. 207.

Rechtsgüter, die nach der Rechtsprechung des BVerfG zu den besonders wichtigen Rechtsgütern zu zählen sind“.³²

Sowohl die Echtzeit-Fernidentifizierung als auch die nachträgliche Fernidentifizierung gemäß § 195 Abs. 2 des Entwurfs bedienen sich der Bild- und Tonaufnahmen, die auf öffentlich zugänglichen Flächen etc. angefertigt werden. In dieser Hinsicht besteht **kein qualitativer Unterschied** der verschiedenen Fernidentifizierungsformen. Der im Hinblick auf den Zeitpunkt der Durchführung der Fernidentifizierung bestehende Unterschied ist im Hinblick auf die Übertragbarkeit der Grundsätze der Rasterfahndung **irrelevant**.

Da § 195 Abs. 2 des Entwurfs keine Gefahr für ein hochrangiges Rechtsgut fordert, wird er den Maßstäben des Bundesverfassungsgerichts nicht gerecht und ist dementsprechend als verfassungswidrig anzusehen.

b) Verstoß gegen Art. 14 Abs. 5 UAbs. 1 der Verordnung (EU) 2024/1689

Sowohl die nachträgliche Fernidentifizierung gemäß § 195 Abs. 2 als auch die gemäß § 195b des Entwurfs verstoßen zudem gegen Art. 14 Abs. 5 UAbs. 1 der Verordnung (EU) 2024/1689.

Art. 14 Abs. 5 UAbs. 1 der Verordnung (EU) 2024/1689 legt fest, dass im Falle des Einsatzes von KI-Systemen im Rahmen der Fernidentifizierung – welcher in sämtlichen Fällen der biometrischen Fernidentifizierung möglich sein soll und praktisch unumgänglich sein wird – **keine Folgemaßnahmen** allein aufgrund des Identifizierungsergebnisses veranlasst werden dürfen, „solange diese Identifizierung nicht von mindestens zwei natürlichen Personen, die die notwendige Kompetenz, Ausbildung und Befugnis besitzen, getrennt überprüft und bestätigt wurde“.

§ 195 Abs. 2 S. 5 des Entwurfs verweist auf § 195c Abs. 1 und 3 des Entwurfs, welcher auch im Rahmen der Fernidentifizierung

³² Drucks. 20/4284 S. 45 f.

gemäß § 195b des Entwurfs zur Anwendung kommt und das Verfahren der Durchführung der Fernidentifizierung regeln soll.

§ 195c Abs. 1 S. 2 des Entwurfs sieht lediglich vor, dass das Ergebnis der Fernidentifizierung, *„bevor weitere polizeiliche Maßnahmen getroffen werden, durch zwei Beschäftigte der Polizei zu überprüfen und zu bestätigen“* ist. Das Erfordernis der Prüfung durch zwei Polizeibeamte, die voneinander getrennt erfolgt, **fehlt**.

2. § 195b des Entwurfs: Fernidentifizierung anhand öffentlich zugänglicher Daten des Internets

§ 195b des Entwurfs soll eine nachträgliche Fernidentifizierung anhand von Vergleichsdaten ermöglichen, die aus öffentlich zugänglichen Daten des Internets gewonnen werden.

Die Datenmenge, auf die hierbei zurückgegriffen werden kann, ist enorm. Aufgrund der Verarbeitung dieser immensen Datenmenge ergibt sich ein Eingriff in die informationelle Selbstbestimmung einer unüberschaubaren Anzahl von Personen. Es werden zum ganz überwiegenden Teil Daten von Personen verarbeitet, die keinen Anlass zur Durchführung der Maßnahme gegeben haben.

Verstoß gegen Art. 5 Abs. 1 lit. e der Verordnung (EU) 2024/1689

Durch diese massenhafte Datenverarbeitung kann ein Gefühl der Massenüberwachung entstehen oder verstärkt werden.³³ Um dem entgegenzuwirken, verbietet **Art. 5 Abs. 1 lit. der Verordnung (EU) 2024/1689** unter anderem *„die Verwendung von KI-Systemen, die **Datenbanken zur Gesichtserkennung** durch das **ungezielte Auslesen von Gesichtsbildern** aus dem Internet [...] erstellen oder erweitern“*. Was hierunter zu verstehen ist, wurde in den **Leitlinien der Kommission** festgelegt.³⁴ Hiergegen verstößt die vorgesehene nachträgliche Fernidentifizierung anhand öffentlich zugänglicher Daten aus dem Internet.

³³ Vgl. Erwägungen 43 zur Verordnung (EU) 2024/1689.

³⁴ Leitlinien der Kommission zu verbotenen Praktiken der künstlichen Intelligenz gemäß der Verordnung (EU) 2024/1689 Rdnr. 226, 228.

a) Erstellen oder Erweitern einer Datenbank

Unter den Begriff der **Datenbank** im Sinne des Art. 5 Abs. 1 lit. e Verordnung (EU) 2024/1689 fällt „jede Sammlung von Daten oder Informationen [...], die speziell für eine schnelle Suche und Abfrage durch einen Computer aufgebaut ist. [...] Eine solche Datenbank zur Gesichtserkennung kann temporär, zentral oder dezentral sein“.³⁵

Durch die explizite Nennung lediglich temporärer Datenbanken wird verdeutlicht, dass **eine unverzügliche Löschung des Entstehens einer Datenbank nicht verhindert**. Die Weiternutzung zu neuen, zukünftigen Anlässen ist für das Eingreifen des Verbots gerade nicht erforderlich.³⁶

Eine Analyse des Wissenschaftlichen Dienstes des Bundestages kam zu dem Ergebnis, dass ein biometrischer Abgleich mit Bildern aus dem Internet ohne die Erstellung oder Verwendung einer Datenbank im Sinne des Art. 5 Abs. 1 lit. e der Verordnung (EU) 2024/1689 nicht möglich ist.³⁷

b) Ungezieltes Auslesen von Gesichtsbildern

Die in § 195b des Entwurfs vorgesehene **Auslese von Gesichtsbildern** erfolgt zudem **ungezielt** im Sinne des Art. 5 Abs. 1 lit. e Verordnung (EU) 2024/1689.

Laut der Leitlinie der Kommission erfolgt eine Auslese ungezielt, wenn „kein besonderer Schwerpunkt auf bestimmte Einzelpersonen oder eine bestimmte Gruppe von Einzelpersonen gelegt wird“.³⁸

Ein solcher Schwerpunkt muss bereits bei der Auslese und nicht erst beim Abgleich gesetzt werden, also schon bei der

³⁵ Leitlinien der Kommission zu verbotenen Praktiken der künstlichen Intelligenz gemäß der Verordnung (EU) 2024/1689 Rdnr. 226.

³⁶ Anders Drucks. 20/4284 S. 59.

³⁷ Deutsche Bundestag – Wissenschaftliche Dienste, Biometrischer Abgleich mit Bildern aus dem Internet, Fachbereiche EU 6 und WD 5, EU 6 - 3000 - 074/25; WD 5 - 3000 - 105/25, S. 16.

³⁸ Leitlinien der Kommission zu verbotenen Praktiken der künstlichen Intelligenz gemäß der Verordnung (EU) 2024/1689, Rdnr. 228.

anfänglichen Gewinnung von Vergleichstemplates. Deren Abgleich mit Referenztemplates in einem zweiten Schritt kann die Zielsetzung der Auslese nicht mehr beeinflussen. Hinsichtlich der Schwerpunktsetzung kann daher nicht auf die Bestätigung der Identität der Person, von der das Referenztemplate stammt, abgestellt werden. Art. 5 Abs. 1 lit. e der Verordnung (EU) 2024/1689 setzt vielmehr voraus, dass bereits der Kreis der Personen, deren Bilder zur Gewinnung von Vergleichstemplates genutzt wird, begrenzt sein muss. Eine solche Begrenzung ist in § 195b Abs. 1 des Entwurfs nicht vorgesehen. Es besteht ein erheblicher Unterschied zwischen der ungezielten Auslese, die Art. 5 Abs. 1 lit. e der Verordnung (EU) 2024/1689 verbietet und der anlasslosen Auslese die durch § 195b des Entwurfs unterbunden wird.³⁹

Die in § 195b des Entwurfs vorgesehene biometrische Fernidentifizierung ermöglicht und erfordert somit die Verwendung von KI-Systemen, die Datenbanken zur Gesichtserkennung durch das ungezielte Auslesen von Gesichtsbildung aus dem Internet erstellen. § 195b des Entwurfs verstößt also gegen Art. 5 Abs. 1 lit. e der Verordnung (EU) 2024/1689.

3. § 184b des Entwurfs: Echtzeit-Fernidentifizierung

Auch die in § 184b des Entwurfs vorgesehene Echtzeit-Fernidentifizierung verstößt gegen europäisches Recht.

Verstoß gegen die Verordnung (EU) 2024/1689

Die in § 184c Abs. 1 S. 2 des Entwurfs, welcher das Verfahren im Rahmen der Echtzeit-Fernidentifizierung regelt, vorgesehene Überprüfung und Bestätigung des Abgleichergebnisses durch zwei qualifizierte Beschäftigte der Polizei genügt nicht den Anforderungen des **Art. 14 Abs. 5 UAbs. 1 der Verordnung (EU) 2024/1689**.

Auch hier fehlt das Erfordernis der getrennten Prüfung.

³⁹ Hierzu Drucks. 20/4284 S. 59.

4. Fazit

Sämtliche vorgesehenen Varianten der biometrischen Fernidentifizierung sind mit höherrangigem Recht unvereinbar. Die vorgesehenen Möglichkeiten der biometrischen Fernidentifizierung sind daher restlos zu streichen.

Prof. Dr. Michael Gubitz, Rechtsanwalt, Fachanwalt für Strafrecht