

Schleswig-Holsteinischer Landtag
Umdruck 20/7149

**AMNESTY
INTERNATIONAL**



An: Herrn Jan Kürschner,
Vorsitzender des Innen- und
Rechtsausschusses,
Landtag von Schleswig-Holstein

STELLUNGNAHME VON AMNESTY INTERNATIONAL ZUM GESETZENTWURF ZUR FORTENTWICKLUNG POLIZEIRECHTLICHER MAßNAHMEN FÜR EINEN WIRKSAMEN SCHUTZ DER ÖFFENTLICHEN SICHERHEIT

Gesetzentwurf der Landesregierung Schleswig-Holstein –
Drucksache 20/4284 und Umdruck 20/6786

Berlin, 11.09.2026



INHALT

I.	Vorbemerkungen und Zusammenfassung	4
II.	Menschenrechtliche Bewertung einzelner Massnahmen	6
1.	Ausbau KI-gestützter Videoüberwachung, § 184 LVwG-E	6
1.1.	Ausweitung der Überwachungsbefugnisse im öffentlichen Raum, § 184 Abs. 3	6
1.1.1.	Hohe Eingriffsintensität und niedrige Eingriffsschwellen	6
1.1.2.	Einschüchterungseffekte	7
1.1.3.	Unzureichende Schutzmechanismen	7
1.2.	Verhaltensscanner, § 184 Abs. 5 LVwG-E	8
1.2.1.	Erhebliche Eingriffsintensität	9
1.2.2.	Risiko von Fehlklassifizierungen und Diskriminierung	10
1.2.3.	Einschüchterungseffekte	11
1.2.4.	Bestimmtheitsdefizite	11
1.2.5.	Unzureichende Schutzmechanismen	12
1.2.6.	Fehlende Wirksamkeitsnachweise	12
2.	Biometrische Fernidentifizierung	13
2.1.	Echtzeit-Fernidentifizierung, §§ 184b, 184c, 186 Abs. 3 und 6 LVwG-E	13
2.1.1.	Erhebliche Eingriffsintensität	13
2.1.2.	Risiko von Fehlidentifikationen und Diskriminierung	14
2.1.3.	Einschüchterungseffekte	15
2.1.4.	Defizite der Normenklarheit	15
2.1.5.	Unzureichende Schutzmechanismen	16
2.1.6.	Fehlende Wirksamkeitsnachweise	17
2.2.	Nachträgliche Fernidentifizierung, §§ 195b, 195c LVwG-E	17
2.2.1.	Erhebliche Eingriffsintensität	17
2.2.2.	Risiko von Fehlidentifikationen, Diskriminierung und Missbrauch	18
2.2.3.	Einschüchterungseffekte	18
2.2.4.	Defizite der Bestimmtheit und der Vereinbarkeit mit der KI-Verordnung	19
2.2.5.	Unzureichende Schutzmechanismen	20
3.	Automatisierte Datenerhebung im öffentlichen Verkehrsraum, § 184d LVwG-E	20
3.1.	Erhebliche Eingriffsintensität und niedrige Eingriffsschwelle	21
3.2.	Unzureichende Schutzmechanismen und Unverhältnismäßigkeit	21
4.	Datenerhebungen mittels mobiler Sensorträgersysteme, § 185e LVwG-E	22
4.1.	Erhebliche Eingriffsintensität	23
4.2.	Unzureichende Schutzmechanismen	23
5.	Automatisierte Datenanalyse, §§ 188c, 188d LVwG-E	24



5.1. Erhebliche Eingriffsintensität	24
5.2. Risiko von Fehltreffern und Diskriminierung	26
5.3. Unzureichende Schutzmechanismen und verbleibende Gefahren	26
6. Ausweitung des Präventivgewahrsams, §§ 204, 205, 205a LVwG-E	27
6.1. Schwerste Eingriffsintensität	27
6.2. Erweiterte Prognoseentscheidungen und Unbestimmtheitsrisiken	28
6.3. Zweifel an der Verhältnismäßigkeit	29
6.4. Unzureichende Schutzmechanismen	30



I. VORBEMERKUNGEN UND ZUSAMMENFASSUNG

Amnesty International in Deutschland bedankt sich für die Möglichkeit zur Stellungnahme und die angemessene Stellungnahmefrist. Amnesty International wird nur zu ausgewählten Regelungen des vorliegenden Gesetzentwurfs Stellung nehmen und behält sich vor, weitere Anmerkungen im Laufe des Gesetzgebungsverfahrens vorzunehmen.

Die folgenden Vorhaben begegnen umfassenden menschenrechtlichen Bedenken und sollten in der vorgesehen Form nicht verabschiedet werden:

- Die **Ausweitung der Videoüberwachung im öffentlichen Raum** senkt die Eingriffsschwellen und erhöht die Streubreite staatlicher Beobachtung. Die vorgesehenen Schutzmechanismen reichen angesichts der Eingriffsintensität nicht aus, zusätzlich fehlt es an Wirksamkeitsnachweisen.
- Die Einführung von **KI-gestützten Verhaltensscannern** ermöglicht die verdachtsunabhängige automatisierte Bewertung und Nachverfolgung des Verhaltens aller Menschen, die sich im öffentlichen Raum bewegen. Wegen erheblicher Fehler-, Diskriminierungs- und Einschüchterungsrisiken, der hohen Streubreite sowie fehlender Wirksamkeitsnachweise sollte auf die Regelung verzichtet werden.
- Die weitreichenden Befugnisse zur **biometrischen Echtzeit- und nachträglichen Fernidentifizierung** heben die Anonymität im öffentlichen und digitalen Raum weitgehend auf. Sie gehen mit erheblichen Fehler-, Diskriminierungs-, Datenschutz- und Rechtsschutzrisiken sowie ebenfalls einer hohen Streubreite einher und begegnen zudem unionsrechtlichen Bedenken.
- Die **automatisierte Datenerhebung und Verhaltensauswertung im öffentlichen Verkehrsraum** erfasst anlasslos eine Vielzahl unbeteiligter Personen, obwohl die Maßnahme lediglich der Verhütung von Ablenkungsverstößen dient. Die niedrige Eingriffsschwelle und die unzureichend bestimmten Voraussetzungen für eine Ausweitung der Kontrolle begründen erhebliche Zweifel an ihrer Verhältnismäßigkeit.
- Der Einsatz **mobiler Sensorträgersysteme, insbesondere von Drohnen**, flexibilisiert und erweitert polizeiliche Überwachung erheblich. Der besonderen Mobilität, Reichweite und eingeschränkten Wahrnehmbarkeit dieser Systeme stehen keine hinreichenden spezifischen Kontroll-, Transparenz- und Dokumentationspflichten gegenüber.
- Die **automatisierte Datenanalyse** ermöglicht die Zusammenführung umfangreicher Datenbestände, die Generierung neuer Erkenntnisse und die Erstellung von **Verhaltensprofilen**, zudem werden personenbezogene Daten einer Vielzahl unbeteiligter Personen verarbeitet. Die vorgesehenen Schutzvorkehrungen begrenzen die Risiken intransparenter Analyseprozesse, fehlerhafter Verdachtsgenerierung, diskriminierender Musterbildung und weitreichender Profilbildung nicht ausreichend.
- Die **Ausweitung des Präventivgewahrsams** senkt die Eingriffsschwelle für den schwersten präventiv-polizeilichen Grundrechtseingriff, erweitert behördliche Prognosespielräume und ermöglicht Freiheitsentziehungen von bis zu zwei Monaten. Die Regelung begegnet erheblichen Bedenken im Hinblick auf das Freiheitsgrundrecht, den Verhältnismäßigkeitsgrundsatz und Art. 5 EMRK.

Amnesty International weist darauf hin, dass der vorliegende Gesetzentwurf mit einer erheblichen Ausweitung und Technisierung polizeilicher Befugnisse in Schleswig-Holstein einhergeht. Videoüberwachung, automatisierte Verhaltensanalyse, biometrische Fernidentifizierung, mobile



Sensorträgersysteme und automatisierte Datenanalyse schaffen eine **zunehmend vernetzte, datengetriebene Überwachungsinfrastruktur**. Die Maßnahmen sind bereits für sich genommen schwerwiegende Grundrechtseingriffe; zusätzlich ergeben sich Auswirkungen auf die freie Wahrnehmung von Grundrechten aber auch aus ihrem **Zusammenwirken**, welches sich in einer Einzelbewertung der jeweiligen Befugnisse regelmäßig nur unvollständig abbilden lässt.

Es besteht die Gefahr einer **schleichenden Normalisierung** schwerwiegender Grundrechtseingriffe, die vielfach und **oftmals sogar vornehmlich auch unbeteiligte Personen** erfassen und **Einschüchterungswirkungen** auf die Wahrnehmung gesellschaftlicher, politischer, kultureller und religiöser Freiheiten entfalten können. Besonders zu berücksichtigen sind die Auswirkungen auf Menschen und Communities, die bereits von Rassismus oder anderen Formen **struktureller Diskriminierung** betroffen sind. Fehlerhafte oder verzerrte automatisierte Bewertungen können bestehende Benachteiligungen reproduzieren oder verstärken und dazu führen, dass Menschen überproportional häufig in den Fokus polizeilicher Maßnahmen geraten.¹

Den schwerwiegenden Grundrechtseingriffen stehen dabei regelmäßig **bloß vermutete Sicherheitsgewinne** gegenüber. Es **fehlen belastbare empirische Erkenntnisse zur Wirksamkeit** entsprechender Maßnahmen, wie sie auch die EU-Grundrechteagentur (FRA) fordert.² Die Einführung weitreichender KI-gestützter Überwachungsbefugnisse für die Polizei darf nicht als **vorschnelle Reaktion auf Sicherheitsdebatten** erfolgen. Vielmehr ist der Staat verpflichtet, bei der Ausgestaltung und Anwendung hoheitlicher Befugnisse die **Grund- und Menschenrechte konsequent zu wahren und zu schützen**.

Erforderlich sind dabei nicht nur **enge, bestimmte und verhältnismäßige gesetzliche Grenzen** sowie **wirksame unabhängige Kontroll- und Rechtsschutzmechanismen**, sondern auch eine **kritische Reflexion bestehender Strukturen, Prozesse und Handlungsmuster** und die **ernsthafte und wirkungsvolle Einbeziehung betroffener Communities**.

Über verwendete technische Systeme sollte **größtmögliche Transparenz** hergestellt werden, um die Nachvollziehbarkeit und Vorhersehbarkeit staatlichen Handels zu verbessern und die Rechtsschutzgarantie aus Art. 19 Abs. 4 GG zu gewährleisten. Der Entwurf ermöglicht die Einführung von KI-Systemen, die als **Hochrisiko-Systeme** im Sinne der Verordnung (EU) 2024/1689 über Künstliche Intelligenz (KI-VO) gelten. Diese sieht beim Einsatz durch Strafverfolgungsbehörden allerdings bloß reduzierte Transparenzvorgaben vor (Art. 49 Abs. 4 KI-VO). Amnesty International empfiehlt, über die Mindestvorgaben der Verordnung für Strafverfolgungsbehörden hinauszugehen. Dazu sollten die Einträge im EU-Transparenzregister gemäß den regulären Vorgaben vorgenommen werden (**Vermerk im öffentlichen Register; vollständige Angaben**) und ein **KI-Transparenzregister** auf Landesebene eingeführt werden.

Bei der Erstellung der nach der Verordnung notwendigen **Grundrechtsfolgenabschätzung** der eingesetzten Systeme sollte die o.g. wirkungsvolle Einbeziehung betroffener Communities berücksichtigt werden.

¹ OHCHR, A/HRC/56/68 (2024); FRA, Facial recognition technology: fundamental rights considerations in the context of law enforcement (2019); FRA, Bias in algorithms – Artificial intelligence and discrimination (2022).

² FRA, Getting the future right – Artificial Intelligence and fundamental rights (2020).



II. MENSCHENRECHTLICHE BEWERTUNG EINZELNER MASSNAHMEN

1. Ausbau KI-gestützter Videoüberwachung, § 184 LVwG-E

1.1. AUSWEITUNG DER ÜBERWACHUNGSBEFUGNISSE IM ÖFFENTLICHEN RAUM, § 184 ABS. 3

Der Entwurf erweitert die Befugnisse zur Videoüberwachung im öffentlichen Raum erheblich. § 184 Abs. 1-3 LVwG-E schafft nicht nur zusätzliche Möglichkeiten der Bild- und Tonaufzeichnung bei öffentlichen Veranstaltungen und Ansammlungen sowie auf allgemein zugänglichen Flächen, sondern ermöglicht künftig auch eine anlassbezogene und kurzfristige Einrichtung von Überwachungsmaßnahmen mittels mobiler Überwachungstechnik. Die **Videoüberwachung** wird damit von fest eingerichteten Standorten gelöst und **räumlich deutlich flexibilisiert**.

§ 184 Abs. 3 LVwG-E verschiebt die Grenzen zulässiger Überwachung im öffentlichen Raum deutlich zulasten der Grund- und Menschenrechte. Die Vorschrift verbindet eine gesteigerte Eingriffsintensität mit abgesenkten Eingriffsschwellen (s. 1.1.1.). Hinzu treten mögliche Einschüchterungs- und Abschreckungseffekte auf die Wahrnehmung gesellschaftlicher, kultureller und politischer Teilhabe im öffentlichen Raum (s. 1.1.2.). Die vorgesehenen Schutzmechanismen vermögen diese Grundrechtsrisiken nur teilweise zu kompensieren, sodass erhebliche Zweifel an der Verhältnismäßigkeit der vorgesehenen Erweiterung bestehen (s. 1.1.3.). Die Regelung sollte daher in ihrer derzeitigen Fassung nicht verabschiedet werden. Jedenfalls bedarf es einer deutlichen Begrenzung des Anwendungsbereichs, präziserer tatbestandlicher Voraussetzungen sowie wirksamerer unabhängiger Kontrollmechanismen.

1.1.1. Hohe Eingriffsintensität und niedrige Eingriffsschwellen

Die in § 184 Abs. 1-3 LVwG-E vorgesehenen Befugnisse zur offenen Video- und Tonüberwachung des öffentlichen Raums stellen einen schweren Eingriff in das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG dar. Die Erhebung, Speicherung und Auswertung von Bild- und Tondaten ermöglicht die Dokumentation von Aufenthalten, Bewegungen und sozialen Interaktionen im öffentlichen Raum und schafft damit die Grundlage für eine **weitreichende staatliche Beobachtung des individuellen Verhaltens**. Der Entwurf weitet den Anwendungsbereich aus, indem er zusätzliche Örtlichkeiten erfasst und die Möglichkeit einer flexiblen sowie kurzfristigen Einrichtung von Überwachungsmaßnahmen einführt.

Vor diesem Hintergrund sind die **niedrigen Eingriffsschwellen** der Vorschrift besonders kritisch. Bereits die in § 184 Abs. 1 und 2 LVwG-E fortgeführten Eingriffsschwellen begegnen grund- und menschenrechtlichen Bedenken. So erlaubt Abs. 1 Datenerhebungen bereits zur Verhütung von Ordnungswidrigkeiten von erheblicher Bedeutung, während Abs. 2 die Beobachtung allgemein zugänglicher Flächen ohne konkrete Gefahr allein zur Erfüllung der polizeilichen Aufgaben nach § 162 LVwG zulässt. Diese Bedenken werden durch den vorliegenden Entwurf jedoch nicht neu geschaffen, sondern bestehen bereits nach geltendem Recht.



Die eigentliche Ausweitung der Überwachungsbefugnisse erfolgt durch die Neufassung des § 184 Abs. 3 LVwG-E. Während offene Videoüberwachung bislang auf Kriminalitäts- und Gefahrenschwerpunkte beschränkt war und Gefahren für Leib, Leben, Freiheit oder vergleichbar gewichtige Rechtsgüter voraussetzte, genügen künftig bereits eine Gefahr für die öffentliche Sicherheit, die Erwartung erheblicher Ordnungswidrigkeiten oder Straftaten oder das Vorliegen eines gefährlichen oder gefährdeten Ortes. Die bisherige **Beschränkung auf Gefahren für besonders gewichtige Rechtsgüter wird damit weitgehend aufgegeben**. Zugleich erweitert der Entwurf die Zahl der überwachten Orte. Der Verweis der Gesetzesbegründung auf die Voraussetzungen des § 181 Abs. 1 bis 3 LVwG-E sowie die Pflicht zur Gefahrenprognose³ vermag hieran nichts zu ändern. Zwar bleiben Prognose- und Dokumentationspflichten bestehen; die materielle Eingriffsschwelle wird gegenüber der bisherigen Rechtslage jedoch deutlich abgesenkt. Die Vorschrift löst sich damit von der bisherigen Konzentration auf Gefahren für besonders gewichtige Rechtsgüter und eröffnet eine **wesentlich weitergehende gefahrenvorsorgende Überwachung des öffentlichen Raums**.

Besonders problematisch ist zudem die erhebliche **Streubreite** der Maßnahme. Die Videoüberwachung erfasst typischerweise nicht nur Personen, die Anlass für die Überwachung geben, sondern zwangsläufig auch eine **Vielzahl unbeteiligter Dritter**, die sich lediglich rechtmäßig am überwachten Ort aufhalten. Das Bundesverfassungsgericht misst derartigen Streuwirkungen bei der Bestimmung des Eingriffsgewichts besondere Bedeutung bei. Danach wird der Grundrechtseingriff in das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) verstärkt, wenn Maßnahmen eine große Zahl unbescholtener Personen erfassen und eine Nutzung öffentlicher Räume nur noch unter den Bedingungen staatlicher Beobachtung ermöglichen.⁴

1.1.2. Einschüchterungseffekte

Zudem bestehen erhebliche Bedenken hinsichtlich möglicher Einschüchterungs- und Abschreckungseffekte (sog. chilling effects) und der damit verbundenen mittelbaren Grundrechtseingriffe.

Wie das Bundesverfassungsgericht betont, kann **bereits die Möglichkeit staatlicher Beobachtung** dazu führen, dass Menschen ihr **Verhalten anpassen** oder auf die Wahrnehmung bestimmter Freiheiten verzichten. Wer nicht hinreichend abschätzen kann, ob und wie Informationen über ihn erfasst und verwendet werden, kann in seiner Freiheit gehemmt werden, von seinen Grundrechten Gebrauch zu machen.⁵

Zwar werden Versammlungen vom Anwendungsbereich der Norm ausgenommen. Die Überwachung wird jedoch auf allgemein zugängliche sowie als gefährlich oder gefährdet eingestufte Orte ausgeweitet, an denen regelmäßig **soziale, kulturelle, religiöse und politische Teilhabe** stattfindet. Zudem können Personen auch auf dem Weg zu oder von einer Versammlung sowie nach deren Beendigung weiterhin von Überwachungsmaßnahmen erfasst werden. Betroffen sind insoweit neben dem Recht auf informationelle Selbstbestimmung mittelbar auch die Meinungsfreiheit aus Art. 5 Abs. 1 GG sowie die Versammlungsfreiheit aus Art. 8 GG.

1.1.3. Unzureichende Schutzmechanismen

Zu begrüßen ist, dass § 184 Abs. 3 S. 3 LVwG-E eine schriftliche Dokumentation der Anordnungsvoraussetzungen vorsieht und die Maßnahme nach § 184 Abs. 3 S. 4 LVwG-E räumlich zu

³ Drucksache 20/4284, S. 40.

⁴ BVerfG, Beschl. v. 18.12.2018, 1 BvR 142/15, BVerfGE 150, 244, Rn. 51, 98.; BVerfG, Urt. v. 16.02.2023, 1 BvR 1547/19, BVerfGE 165, 363, Rn. 95ff.

⁵ BVerfG, Urt. vom 15.12.1983, 1 BvR 209/83, BVerfGE 65, 1, Rn. 146.



beschränken sowie auf sechs Monate zu befristen ist. Hinzu treten die Löschungs- und Dokumentationspflichten des § 184 Abs. 6 LVwG-E sowie die Hinweispflichten des § 184 Abs. 7 LVwG-E.

Die Schutzwirkung dieser Vorgaben bleibt jedoch begrenzt. Insbesondere verbleiben die Entscheidung über die Anordnung der Maßnahmen, deren Verlängerung sowie die weitere Speicherung der erhobenen Daten weitgehend **innerhalb der behördlichen Eigenkontrolle**. Das Bundesverfassungsgericht betont jedoch wiederholt, dass mit zunehmender Eingriffsintensität die Anforderungen an Begrenzung, Transparenz, Kontrolle und verfahrensrechtliche Absicherung staatlicher Überwachungsmaßnahmen steigen und gerade verfahrensrechtliche Sicherungen eine eigenständige grundrechtsschützende Funktion erfüllen.⁶

Hinzu kommt, dass die Gesetzesbegründung die Ausweitung maßgeblich mit positiven Erfahrungen an einzelnen überwachten Orten begründet.⁷ Aus lokalen Rückgängen von Gewalttaten, Diebstählen oder Sachbeschädigungen lässt sich jedoch nicht ohne Weiteres ableiten, dass eine landesweite Ausweitung der Videoüberwachung bei abgesenkten Eingriffsschwellen erforderlich und verhältnismäßig ist. Insbesondere wird **nicht dargelegt, ob die beobachteten Effekte dauerhaft waren, auf die Überwachung selbst zurückzuführen sind und ob sie lediglich zu Verlagerungseffekten geführt haben**. Der Verweis auf einzelne positive Erfahrungen ersetzt keine eigenständige Begründung dafür, weshalb die bisherige Rechtslage nicht ausreicht und die nun vorgesehene Erweiterung der Überwachungsbefugnisse erforderlich sein soll.

Schließlich sind Bild- und Tonaufzeichnungen grundsätzlich nach einem Monat zu löschen. § 184 Abs. 6 S. 2 LVwG-E eröffnet jedoch **weitreichende Ausnahmen von dieser Löschungspflicht**. Eine längere Speicherung ist bereits zulässig, wenn die Aufzeichnungen zur Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung oder Straftaten benötigt werden, wenn sie zur vorbeugenden Aufgabenerfüllung weiterhin erforderlich erscheinen oder wenn mit einer Überprüfung der Rechtmäßigkeit der Maßnahme zu rechnen ist. Die gesetzliche Regelung ermöglicht damit eine erhebliche Verlängerung der Datenvorhaltung über den eigentlichen Erhebungszweck hinaus.

Vor diesem Hintergrund bestehen Zweifel, ob die im Entwurf vorgesehenen Schutzvorkehrungen in einem angemessenen Verhältnis zur erheblichen Erweiterung der Überwachungsbefugnisse stehen.

1.2. VERHALTENSSCANNER, § 184 ABS. 5 LVWG-E

Mit § 184 Abs. 5 LVwG-E wird erstmals eine Rechtsgrundlage für den Einsatz sogenannter Verhaltensscanner geschaffen. Die Vorschrift erlaubt die automatisierte Analyse von Videoüberwachungsdaten auf Bewegungs- und Verhaltensmuster, die auf Gefahren für Leben, Leib, Freiheit oder die sexuelle Selbstbestimmung hindeuten können. Vorgesehen ist ein zweistufiges Verfahren: Zunächst werden potenziell gefahrrelevante Muster automatisiert erkannt und dann einer menschlichen Prüfung unterzogen. Wird der Verdacht bestätigt, kann die betroffene Person anschließend in Bildübertragungen, Bildaufnahmen oder Bildaufzeichnungen automatisiert gekennzeichnet und über mehrere Kameras hinweg nachverfolgt werden. Die Regelung ermöglicht damit nicht nur eine **automatisierte Verhaltensanalyse**, sondern auch ein **kameraübergreifendes Tracking von Personen im öffentlichen Raum**. Auch wenn nach dieser Vorschrift eine biometrische Identifizierung ausgeschlossen ist (s. dazu 2.), geht sie qualitativ deutlich über die klassische Videoüberwachung hinaus und eröffnet neue Formen KI-gestützter Überwachung und Verhaltensauswertung.

§ 184 Abs. 5 LVwG-E markiert einen **Paradigmenwechsel von der Beobachtung hin zur automatisierten Bewertung menschlichen Verhaltens im öffentlichen Raum**. Die Vorschrift ermöglicht die **verdachtsunabhängige** algorithmische Analyse aller Personen im betroffenen Raum und schafft damit die

⁶ BVerfG, Urt. v. 20.04.2016, 1 BvR 966/09, BVerfGE 141, 220, Rn. 136 ff., 220 ff.; BVerfG, Urt. v. 16.02.2023, 1 BvR 1547/19, BVerfGE 165, 363, Rn. 90 ff., 112 ff., 115 ff.

⁷ Drucksache 20/4284, S. 40.



Grundlage für eine neue Qualität staatlicher Überwachung. Die Kombination aus erheblicher Eingriffsintensität (s. 1.2.1.), Fehlklassifizierungs- und Diskriminierungsrisiken (s. 1.2.2.), Einschüchterungseffekten (s. 1.2.3.), erheblichen Bestimmtheitsdefiziten (s. 1.2.4.), unzureichenden Schutzmechanismen (s. 1.2.5.) und fehlenden Wirksamkeitsnachweisen (s. 1.2.6.) begegnet schwerwiegenden grund- und menschenrechtlichen Bedenken. Die Regelung sollte daher nicht verabschiedet werden.

1.2.1. Erhebliche Eingriffsintensität

Die in § 184 Abs. 5 LVwG-E vorgesehene automatisierte Verhaltensanalyse geht qualitativ deutlich über eine klassische Videoüberwachung hinaus. Sämtliche sich im überwachten öffentlichen Raum aufhaltenden Personen werden automatisiert analysiert, kategorisiert und hinsichtlich eines Gefahrenpotenzials bewertet. Der Eingriff liegt folglich nicht allein in der Datenerhebung, sondern auch in der **technischen Interpretation menschlichen Verhaltens**. Berührt ist das Recht auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG.

Verstärkt wird die Eingriffsintensität durch die in § 184 Abs. 5 S. 3 LVwG-E vorgesehene **automatisierte Nachverfolgung** als gefahrrelevant eingestufte Personen. Die automatisierte Kennzeichnung ermöglicht eine kameraübergreifende Verfolgung im öffentlichen Raum und nähert sich damit funktional einer **Bewegungsprofilbildung** an.

Besonders kritisch ist zudem, dass § 184 Abs. 5 LVwG-E die **staatliche Beobachtung in das Vorfeld konkreter Gefahren** verlagert. Die automatisierte Verhaltensanalyse dient nicht der Überprüfung bereits bestehender Verdachtsmomente, sondern ihrer **erstmaligen Generierung**. Die Maßnahme beruht auf einer flächendeckenden Analyse auch solcher Personen, gegen die keinerlei Verdacht besteht. Diese **erhebliche Streubreite** verstärkt das Gewicht des Eingriffs in das Recht auf informationelle Selbstbestimmung erheblich.

Ferner erfolgt die automatisierte Verhaltensanalyse für die betroffenen Personen nicht unmittelbar wahrnehmbar. Es ist zwar gesondert auf den Einsatz des Systems hinzuweisen (§ 184 Abs. 7 S. 3 LVwG-E), Betroffene haben jedoch regelmäßig **keine Möglichkeit nachzuvollziehen, welche Verhaltensweisen als auffällig definiert wurden, nach welchen Kriterien die Auswertung erfolgt, weshalb eine bestimmte Situation einen automatisierten Treffer ausgelöst hat oder ob sie gerade Objekt einer kameraübergreifenden Nachverfolgung sind**. Die damit verbundene Intransparenz erschwert die Kontrolle der Maßnahme und die Inanspruchnahme effektiven Rechtsschutzes. Zugleich erhöht sie das Gefühl einer unbestimmten und nicht vorhersehbaren Überwachung und verstärkt damit das Eingriffsgewicht.⁸

Schließlich kann § 184 Abs. 5 LVwG-E nicht isoliert betrachtet werden. Die automatisierte Verhaltensanalyse dient gerade dazu, einzelne Personen aus einer Vielzahl erfasster Personen herauszufiltern und einer intensiveren Überwachung zugänglich zu machen. Sie bildet damit faktisch eine **Vorstufe weitergehender Identifizierungs- und Überwachungsmaßnahmen**, insbesondere der biometrischen Fernidentifizierung nach §§ 184b, 184c, 195, 195b, 195c LVwG-E. Die vermeintliche Beschränkung auf eine bloße Mustererkennung relativiert sich dadurch erheblich. Tatsächlich schafft die Vorschrift die **technische Grundlage für eine verdachtsunabhängige Selektion von Personen**, die anschließend zum Gegenstand weiterer Überwachungs- und Identifizierungsmaßnahmen sowie sonstiger polizeilicher Maßnahmen werden können.

⁸ BVerfG, Urt. vom 15.12.1983, 1 BvR 209/83, BVerfGE 65, 1, Rn. 147 f.; BVerfG, Urt. v. 16.02.2023, 1 BvR 1547/19, BVerfGE 165, 363, Rn. 90 ff., 115 ff.



1.2.2. Risiko von Fehlklassifizierungen und Diskriminierung

Wie auch ein Bericht der EU-Grundrechteagentur betont, können KI-Systeme bestehende gesellschaftliche Ungleichheiten reproduzieren oder verstärken. Verzerrungen können bereits in den Trainingsdaten angelegt sein, aus gesellschaftlichen Vorbedingungen resultieren, durch die Auswahl der Modellparameter entstehen oder sich erst im praktischen Einsatz und durch Rückkopplungseffekte entwickeln.⁹

Die UN-Sonderberichterstatterin für zeitgenössische Formen von Rassismus hebt hervor, dass KI-Anwendungen im Bereich staatlicher Überwachung und Strafverfolgung besonders risikobehaftet sind, da Fehlklassifizierungen und diskriminierende Entscheidungen hier unmittelbar in Grund- und Freiheitsrechte eingreifen können.¹⁰

Verhaltensscanner treffen Wahrscheinlichkeitsaussagen und können **alltägliche oder sozial übliche Verhaltensweisen fälschlicherweise als gefahrrelevant einstufen**. Aus Mannheim ist bekannt, dass vergleichbare Systeme nicht nur Verhaltensweisen wie „Schläge“ oder „Tritte“ erkennen sollen, sondern zur Abgrenzung hiervon auch Muster wie „Tanzen“ oder „Umarmen“ auswerten.¹¹ Die Abgrenzung zwischen gefahrrelevantem und alltäglichem Verhalten ist technisch keineswegs eindeutig.

Hinzu kommt, dass vergleichbare Systeme (in Hamburg und Berlin) auch auf Verhaltensweisen wie „Liegen“ reagieren sollen, um auf mögliche Notsituationen aufmerksam zu machen.¹² Gerade an Orten, an denen sich regelmäßig wohnungslose Menschen aufhalten, besteht dadurch das Risiko, dass bestimmte Personengruppen häufiger von automatisierten Alarmierungen und nachfolgenden Kontrollmaßnahmen betroffen sind. Vor diesem Hintergrund bestehen erhebliche Zweifel, ob die **diskriminierungsrelevanten Risiken** der automatisierten Verhaltensbewertung durch die derzeit vorgesehenen gesetzlichen Sicherungen ausreichend beherrscht werden.

Die vorgesehene **menschliche Überprüfung** automatisierter Treffer vermag die grundrechtlichen Bedenken nicht aufzufangen. Sie erfolgt erst nach der automatisierten Analyse der Bilddaten und setzt damit an einem Zeitpunkt ein, zu dem der Eingriff in das Recht auf informationelle Selbstbestimmung bereits verwirklicht ist.¹³ Zwar kann die nachgelagerte Kontrolle Fehlbewertungen reduzieren; sie beseitigt jedoch nicht die grundrechtliche Relevanz der vorgelagerten automatisierten Verarbeitung. Zudem wird die spätere menschliche Bewertung durch die technischen Parameter, Trainingsdaten und Bewertungskriterien des eingesetzten Systems maßgeblich **vorstrukturiert**.

Zusätzlich besteht die Gefahr eines sogenannten **Automation Bias**. Darunter wird die empirisch vielfach nachgewiesene Tendenz verstanden, automatisierten Bewertungen ein besonderes Vertrauen entgegenzubringen und ihre Ergebnisse unkritisch zu übernehmen.¹⁴ Die menschliche Prüfung erfolgt erst, nachdem das System ein Verhalten bereits als potenziell gefahrrelevant eingestuft hat. Die Bewertung durch die Polizeibeschäftigten findet damit nicht unbeeinflusst statt, sondern unter dem Eindruck einer bereits vorhandenen algorithmischen Verdachtskennzeichnung. Dies kann die Gefahr erhöhen, dass

⁹ FRA, Bias in Algorithms: Artificial Intelligence and Discrimination (2022).

¹⁰ OHCHR, A/HRC/56/68 (2024).

¹¹ <https://netzpolitik.org/2026/verhaltensscanner-eine-reale-gefahr/?replytocom=2600045>; <https://netzpolitik.org/2026/software-zur-ueberwachung-berlins-ausgewaehlt-verhaltensscanner-am-kotti-startet-noch-im-sommer/>.

¹² <https://netzpolitik.org/2026/software-zur-ueberwachung-berlins-ausgewaehlt-verhaltensscanner-am-kotti-startet-noch-im-sommer/>.

¹³ BVerfG, Urt. v. 16.02.2023, 1 BvR 1547/19, BVerfGE 165, 363, 50ff.;

BVerfG, Urt. v. 11.03.2008, 1 BvR 2074/05, BVerfGE 120, 378, Rn. 66 ff.

¹⁴ Romeo / Conti, *Exploring automation bias in human-AI collaboration: a review and implications for explainable AI*, in: AI & Society 41 (2026), S. 259-278; Ruschemeier / Hondrich, *Automation bias in public administration: An interdisciplinary perspective from law and psychology*, Government Information Quarterly 41 (2024), Art. 101953.



Fehlklassifizierungen des Systems fortwirken und automatisierte Bewertungen faktisch ein größeres Gewicht erhalten, als ihnen aufgrund ihrer Fehleranfälligkeit zukommen sollte.

Weder § 184 Abs. 5 LVwG-E noch die Gesetzesbegründung enthalten Vorgaben zu zulässigen **Fehlerraten**. In Berlin wurde im Rahmen einer Ausschreibung für vergleichbare Systeme zuletzt eine Fehlerrate von bis zu 25 Prozent genannt.¹⁵ Bei einer polizeiinternen Evaluation der Verhaltensscanner am Hamburger Hansaplatz wurden von 1416 Hinweisen des Systems **weniger als 1%** als polizeilich relevant eingestuft.¹⁶ Auch nach den Erwartungen der Polizei kann ein erheblicher Anteil automatisierter Treffer Verhaltensweisen betreffen, die sich im Nachhinein als unproblematisch erweisen. Bereits die automatisierte Markierung einer Person führt jedoch dazu, dass diese **in den Fokus polizeilicher Aufmerksamkeit** gerät und potenziell Gegenstand **weiterer Maßnahmen** wird.

Zudem legen weder Norm noch Gesetzesbegründung nachvollziehbar dar, wie die Systeme trainiert und validiert werden und mit welchen Verfahren mögliche Verzerrungen oder diskriminierende Effekte erkannt und vermindert werden sollen, wodurch erhebliche Risiken für das Gleichbehandlungsgebot des Art. 3 GG sowie das Diskriminierungsverbot nach Art. 14 EMRK entstehen.

Die Gesetzesbegründung verweist zwar darauf, dass die automatisierte Mustererkennung eine „vorurteilsfreie Situationseinschätzung“ ermöglichen und diskriminierende Zuschreibungen verhindern solle.¹⁷ Aus dem Ziel diskriminierungsfreier Entscheidungen folgt jedoch nicht, dass die eingesetzten Systeme tatsächlich frei von diskriminierenden Effekten sind. **Die Behauptung einer vorurteilsfreien Bewertung ersetzt daher keine nachvollziehbare Darlegung, wie Fehlklassifizierungen und mittelbare Diskriminierungen tatsächlich verhindert werden sollen.**

1.2.3. Einschüchterungseffekte

Darüber hinaus birgt die Vorschrift das Risiko erheblicher Einschüchterungs- und Anpassungseffekte (chilling effects, s. 1.1.2.). Über klassische Videoüberwachung hinausgehend werden nicht lediglich einzelne Handlungen beobachtet, sondern Verhaltensweisen systematisch auf Auffälligkeiten und Gefahrenindikatoren untersucht, was den **Effekt potenzieren** kann. Auch hier sind daher auch die Meinungsfreiheit (Art. 5 Abs. 1 GG) sowie die Versammlungsfreiheit (Art. 8 GG) betroffen.

1.2.4. Bestimmtheitsdefizite

Ferner begegnet die Vorschrift erheblichen **Bestimmtheitsbedenken**. § 184 Abs. 5 LVwG-E erlaubt die automatisierte Erkennung von „**Bewegungsmustern**“, die auf Handlungen hindeuten sollen, durch welche Leben, Leib, Freiheit oder die sexuelle Selbstbestimmung einer Person beeinträchtigt werden könnten. Weder der Normtext noch die Gesetzesbegründung konkretisieren jedoch hinreichend, welche Verhaltensweisen, Bewegungsabläufe oder sonstigen Indikatoren hierunter fallen sollen. Damit bleibt weitgehend **offen, anhand welcher Kriterien menschliches Verhalten als auffällig oder gefahrrelevant eingestuft** und potenziell einer kameraübergreifenden Nachverfolgung oder weiteren polizeilichen Folgemaßnahmen unterworfen wird. Die eigentliche Konkretisierung der Eingriffsvoraussetzungen wird faktisch auf die technische Ausgestaltung der Systeme, ihre Programmierung und die Festlegung der verwendeten Parameter verlagert. Für die Betroffenen ist daher **kaum vorhersehbar**, welches Verhalten eine automatisierte Erfassung, Markierung oder polizeiliche Reaktion auslösen kann. Dies erscheint insbesondere deshalb problematisch, weil das Bundesverfassungsgericht gerade bei grundrechtsintensiven informationellen Überwachungsmaßnahmen hohe Anforderungen an Normenklarheit, Vorhersehbarkeit und

¹⁵ <https://taz.de/KI-Videoeueberwachung-in-Berlin/!6160851/>.

¹⁶ <https://marx.wtf/2024/12/24/der-hansaplatz-versuch-war-kein-erfolg/>.

¹⁷ Drucksache 20/4284, S. 41.



die gesetzliche Begrenzung der Datenverarbeitung stellt. Je stärker die Maßnahme in Freiheitsrechte eingreift, desto präziser müssen ihre Voraussetzungen gesetzlich festgelegt sein.¹⁸ Diesen Anforderungen wird § 184 Abs. 5 LVwG-E nicht vollständig gerecht. Dies erschwert zugleich die gerichtliche Kontrolle der Maßnahme und erhöht das Risiko uneinheitlicher, fehlerhafter oder unverhältnismäßiger Eingriffe in die betroffenen Rechte.

1.2.5. Unzureichende Schutzmechanismen

Die Vorschrift enthält zwar einzelne Sicherungen, insbesondere das Verbot einer automatisierten biometrischen Identifizierung auf Grundlage der Vorschrift (§ 184 Abs. 5 S. 4 Halbs. 2 LVwG-E), die verpflichtende nachgelagerte Überprüfung automatisierter Treffer durch qualifizierte Polizeibeschäftigte (§ 184 Abs. 5 S. 2 LVwG-E), die Löschungsregelungen des § 184 Abs. 6 LVwG-E (hierzu aber bereits 1.1.3.) sowie die Dokumentations- und Transparenzpflichten nach § 184 Abs. 6 S. 3 und § 184 Abs. 7 S. 3 LVwG-E. Nach der Konzeption des Entwurfs sollen erkannte Bewegungsmuster zudem nicht gespeichert werden (§ 184 Abs. 6 S. 1 LVwG-E).

Diese Vorkehrungen vermögen die Grundrechtsrisiken jedoch nur begrenzt abzumildern.

Wie bereits unter 1.2.1. ausgeführt, gilt das Verbot biometrischer Identifizierung nur für die Verhaltensanalyse selbst. Der Gesetzentwurf schafft jedoch zugleich eigenständige Befugnisse zur biometrischen Fernidentifizierung, sodass **innerhalb desselben Überwachungssystems automatisierte Verhaltensanalysen und biometrische Identifizierungsmaßnahmen** dennoch **funktional aufeinander bezogen eingesetzt** werden können.

Schließlich fehlt es an einer **unabhängigen vorgelagerten Kontrolle**. Weder der Einsatz automatisierter Verhaltensscanner selbst noch die Festlegung der ihnen zugrunde liegenden Suchparameter, Gefahrenindikatoren und Bewertungskriterien bedürfen einer gerichtlichen oder sonstigen unabhängigen Genehmigung. Es fehlen damit gerade diejenigen externen Kontrollmechanismen, denen das Bundesverfassungsgericht bei besonders eingriffsintensiven Überwachungsbefugnissen eine wichtige grundrechtssichernde Funktion beimisst.¹⁹

1.2.6. Fehlende Wirksamkeitsnachweise

Schließlich bestehen Zweifel an der Erforderlichkeit der Neuregelung. Nach dem Grundsatz der **Verhältnismäßigkeit** genügt es nicht, dass eine Maßnahme theoretisch zur Förderung der öffentlichen Sicherheit beitragen kann. Vielmehr muss nachvollziehbar begründet werden, dass von ihr ein tatsächlicher und relevanter Sicherheitsgewinn zu erwarten ist. Auch die EU-Grundrechteagentur fordert, dass der Einsatz von KI-Systemen auf **robuster Evidenz** beruhen muss und dass für grundrechtsrelevante KI-Anwendungen belastbare Nachweise ihrer Auswirkungen erforderlich sind.²⁰ Dies muss im besonderen Maße für KI-gestützte Verhaltensscanner gelten, die das Verhalten sämtlicher erfasster Personen automatisiert analysieren und damit mit erheblichen Grundrechtseingriffen verbunden sind. **Weder der Gesetzentwurf noch seine Begründung legen jedoch belastbare empirische Erkenntnisse zur Wirksamkeit, Trefferquote oder Fehleranfälligkeit solcher Systeme vor.** Fehlt es aber an einer tragfähigen Tatsachengrundlage für den behaupteten Sicherheitsgewinn, gewinnt das Gewicht der betroffenen Freiheitsrechte umso mehr an Bedeutung.

¹⁸ BVerfG, Urt. vom 20.04.2016, 1 BvR 966/09, BVerfGE 141, 220, Rn. 209 ff., 220 ff.; BVerfG, Urt. vom 16.02.2023, 1 BvR 1547/19, BVerfGE 165, 363, insb. Rn. 90 ff., 115 ff.

¹⁹ BVerfG, Urt. vom 20.04.2016, 1 BvR 966/09, BVerfGE 141, 220; BVerfG, Urt. v. 16.02.2023, 1 BvR 1547/19, BVerfGE 165, 363, Rn. 90 ff., 112 ff., 115 ff.

²⁰ FRA, Getting the future right – Artificial Intelligence and fundamental rights (2020).



2. Biometrische Fernidentifizierung

2.1. ECHTZEIT-FERNIDENTIFIZIERUNG, §§ 184B, 184C, 186 ABS. 3 UND 6 LVWG-E

Die Einführung der biometrischen Echtzeit-Fernidentifizierung nach §§ 184b, 184c LVWG-E markiert einen **qualitativen Sprung staatlicher Überwachungsbefugnisse**. Erstmals soll die Polizei Personen im öffentlichen Raum anhand von Gesichts- oder Stimmerkennungsmerkmalen automatisiert und nahezu verzögerungsfrei identifizieren können. Die auf Grundlage der Videoüberwachung nach § 184 LVWG-E gewonnenen Bild- und Tondaten werden hierfür fortlaufend mit biometrischen Referenzdaten abgeglichen. Die Maßnahme ermöglicht damit einen **Live-Abgleich sämtlicher im Erfassungsbereich befindlicher Personen** und stellt eine der grundrechtsintensivsten Formen polizeilicher Datenverarbeitung dar. Der Gesetzentwurf orientiert sich dabei ausdrücklich an den Vorgaben der Verordnung (EU) 2024/1689 über Künstliche Intelligenz (KI-VO), welche die biometrische Echtzeit-Fernidentifizierung aus gutem Grund als besonders eingriffsintensive Technologie, deren **Einsatz grundsätzlich verboten** und nur unter engen Ausnahmeveraussetzungen zulässig ist, behandelt.

§§ 184b, 184c LVWG-E schaffen die weitreichendste Überwachungsbefugnis des gesamten Gesetzentwurfs. Die biometrische Echtzeit-Fernidentifizierung hebt die Anonymität im öffentlichen Raum weitgehend auf und ermöglicht die automatisierte Identifizierung von Personen aus der Ferne. Sie stellt nach Ansicht von Amnesty International **bereits unabhängig von der konkreten Ausgestaltung einen unverhältnismäßigen Eingriff in die informationelle Selbstbestimmung und ein unvertretbares Risiko für weitere Menschenrechte** dar. Die Kombination aus erheblicher Eingriffsintensität (s. 2.1.1.), Fehler- und Diskriminierungsrisiken (s. 2.1.2.), Einschüchterungseffekten (s. 2.1.3.), Defizite in der Normenklarheit (s. 2.1.4.) sowie nur begrenzt wirksamen Schutzmechanismen (s. 2.1.5.) und fehlenden Wirksamkeitsnachweisen (s. 2.1.6.) begegnet schwerwiegenden grund- und menschenrechtlichen Bedenken. Die Regelung sollte daher nicht verabschiedet werden.

2.1.1. Erhebliche Eingriffsintensität

Die biometrische Echtzeit-Fernidentifizierung greift besonders tief in das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) ein. Dies ergibt sich bereits aus der Natur der verarbeiteten Daten. **Biometrische Merkmale zählen zu den sensibelsten Kategorien personenbezogener Daten**. Sie ermöglichen die eindeutige Identifizierung einer Person anhand körperlicher, physiologischer oder verhaltensbezogener Eigenschaften und sind zugleich weitgehend unveränderlich.²¹ Bereits die Gesetzesbegründung erkennt an, dass der zustimmungsfreie biometrische Fernabgleich wegen der Unveränderlichkeit biometrischer Merkmale mit einer besonderen grundrechtlichen Gefährdungslage verbunden ist.²²

Hinzu kommt, dass die Identifizierung aus der Distanz sowie **ohne Wissen und Mitwirkung** der betroffenen Person erfolgen kann. Dadurch unterscheidet sich die biometrische Echtzeit-Fernidentifizierung grundlegend von herkömmlichen Identifizierungsmaßnahmen.

Die Maßnahme beschränkt sich nicht auf die Beobachtung öffentlicher Räume, sondern ermöglicht die Zuordnung beobachteter Verhaltensweisen zu konkreten Personen in Echtzeit. In einem **freiheitlichen Gemeinwesen** gehört jedoch die Möglichkeit, das eigene Gesicht im öffentlichen Raum zu zeigen, ohne

²¹ Coombe/Roth-Isigkeit: Biometrische Fernidentifizierung im Spiegel der KI-Verordnung (ZfDR 2024, 392).

²² Drucksache 20/4284, S. 45f.



jederzeit automatisiert identifiziert werden zu können, zu den grundlegenden Voraussetzungen persönlicher Freiheit.²³

Die besondere Eingriffsintensität ergibt sich schließlich auch aus der **erheblichen Streubreite** der Maßnahme. Die gesuchte Person kann nur gefunden werden, indem die biometrischen Merkmale sämtlicher im Erfassungsbereich befindlicher Personen erfasst und abgeglichen werden. Der Grundrechtseingriff trifft damit überwiegend völlig unbeteiligte Personen. Das Bundesverfassungsgericht hat gerade diese anlasslose Einbeziehung Unbeteiligter als besonderes Merkmal eingriffsintensiver Datenverarbeitungsmaßnahmen hervorgehoben.²⁴

Die massive Grundrechtsrelevanz biometrischer Fernidentifizierung wird auch durch die Position der europäischen Datenschutzaufsichtsbehörden unterstrichen. EDPB und EDPS haben ebenso wie Amnesty International und andere Menschenrechtsorganisationen im Gesetzgebungsverfahren zur KI-Verordnung ein **Verbot biometrischer Fernidentifizierung in öffentlich zugänglichen Räumen** gefordert, da diese Technologie tief in Privatsphäre, Anonymität und weitere Freiheitsrechte eingreift.²⁵ Auch ein Bericht des UN-Hochkommissariats für Menschenrechte hebt biometrische Fernidentifizierungssysteme, insbesondere Gesichtserkennung im öffentlichen Raum, als besonders eingriffsintensive Technologien hervor.²⁶

2.1.2. Risiko von Fehlidentifikationen und Diskriminierung

Das Eingriffsgewicht der biometrischen Echtzeit-Fernidentifizierung wird zusätzlich durch das Risiko fehlerhafter und diskriminierender Identifizierungen erhöht. Zwar unterliegen entsprechende Systeme als Hochrisiko-KI-Systeme besonderen technischen und organisatorischen Anforderungen und ihre Ergebnisse müssen vor weiteren Maßnahmen überprüft werden. Diese Schutzvorkehrungen begrenzen das Risiko von fehlerhaften Zuordnungen jedoch lediglich, ohne es gänzlich auszuschließen.

Nach Erkenntnissen der EU-Grundrechteagentur weisen Gesichtserkennungssysteme teilweise je nach Alter, Geschlecht oder ethnischer Herkunft unterschiedliche Fehlerraten auf, sodass **bestimmte Personengruppen einem erhöhten Risiko von Fehlidentifizierungen** und daraus resultierenden polizeilichen Maßnahmen ausgesetzt sein können.²⁷ Die KI-Verordnung hebt diese Risiken ausdrücklich hervor und unterwirft biometrische Fernidentifizierung deshalb besonders strengen Vorgaben.²⁸

Zwar werden automatisierte Treffer nach § 184c Abs. 1 S. 2 LVwG-E vor weiteren Maßnahmen menschlich überprüft. Wie bereits unter 1.2.2. ausgeführt, ist der Grundrechtseingriff durch die Erfassung, Verarbeitung und den biometrischen Abgleich der Daten zu diesem Zeitpunkt jedoch **bereits erfolgt**. Zudem schließt die nachgelagerte Überprüfung Fehlidentifikationen nicht vollständig aus. Insbesondere besteht auch hier die Gefahr von **Automation Bias**, also der empirisch belegten Tendenz, automatisierten Systemen besonderes Vertrauen entgegenzubringen und ihre Ergebnisse unkritisch zu übernehmen.

Darüber hinaus bestehen erhebliche Risiken im Zusammenhang mit der **Sicherheit biometrischer Daten**. Anders als Passwörter oder sonstige Identifikationsmerkmale können biometrische Merkmale kaum geändert werden. Werden solche Daten unrechtmäßig offengelegt, missbräuchlich verwendet oder durch Cyberangriffe erlangt, kann der betroffene Personenkreis die Kompromittierung seiner biometrischen Merkmale regelmäßig nicht durch einen Austausch oder eine Änderung der Daten kompensieren. Vor dem

²³ Coombe/Roth-Isigkeit: Biometrische Fernidentifizierung im Spiegel der KI-Verordnung, ZfDR 2024, 391, 392.

²⁴ BVerfG, Beschl. vom 4.4.2006, 1 BvR 518/02, BVerfGE 115, 320, Rn. 115ff.

²⁵ EDPB und EDPS, Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), S. 11f.

²⁶ OHCHR, A/HRC/48/31: The right to privacy in the digital age (2021).

²⁷ FRA, *Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement*, 2019, S. 10, 27 f., 33 f.

²⁸ ErwG 32 KI-VO; Art. 5 Abs. 1 lit. h, Abs. 2-7, Art 10, 14, 15 KI-VO; Drucksache. 20/4284, S. 32.



Hintergrund steigender Cyberangriffe auf öffentliche Stellen kommt der Sicherheit biometrischer Daten eine besondere Bedeutung zu.

2.1.3. Einschüchterungseffekte

Bereits die Möglichkeit, im öffentlichen Raum automatisiert identifiziert werden zu können, kann zu Einschüchterungseffekten (chilling effects, s. 1.1.2) führen. Bürger*innen könnten von **der Teilnahme an Veranstaltungen oder anderen Formen gesellschaftlicher und politischer Teilhabe** Abstand nehmen, bestimmte **Orte** (etwa eine Schwangerschaftskonflikt- oder Drogenberatung, ein Partei- oder Gewerkschaftsbüro) oder Formen gesellschaftlicher und politischer Teilhabe meiden. Zwar sind Versammlungen, sofern sie dem Versammlungsgesetz unterliegen, aufgrund des Verweises in § 184b Abs. 1 auf § 184 Abs. 1 LVwG-E von der Echtzeit-Fernidentifizierung ausgenommen. Da Personen auf dem Weg zu oder von einer Versammlung sowie nach deren Beendigung weiterhin von Überwachungsmaßnahmen erfasst werden können, kann die Möglichkeit einer staatlichen Identifizierung dennoch auch die Wahrnehmung der **Versammlungsfreiheit** beeinträchtigen.

Diese Gefahr wird auch vom europäischen Gesetzgeber ausdrücklich anerkannt. Im Erwägungsgrund 32 zur KI-VO dort heißt es:

*„Die Verwendung von KI-Systemen zur biometrischen Echtzeit-Fernidentifizierung natürlicher Personen in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken greift besonders in die Rechte und Freiheiten der betroffenen Personen ein, da sie die Privatsphäre eines großen Teils der Bevölkerung beeinträchtigt, ein **Gefühl der ständigen Überwachung** weckt und **indirekt von der Ausübung der Versammlungsfreiheit und anderer Grundrechte abhalten** kann. Technische Ungenauigkeiten von KI-Systemen, die für die biometrische Fernidentifizierung natürlicher Personen bestimmt sind, können zu verzerrten Ergebnissen führen und eine **diskriminierende Wirkung** haben.“*

Auch der UN-Hochkommissar für Menschenrechte zählt Einschüchterungs- und Abschreckungseffekte zu den zentralen Risiken KI-gestützter Überwachungs- und Analysensysteme. Die Aussicht, fortlaufend algorithmisch bewertet zu werden, birgt die Gefahr von Verhaltensanpassungen und Selbstzensur und kann damit die freie Wahrnehmung von Meinungs-, Versammlungs- und Teilhaberechten beeinträchtigen.²⁹

2.1.4. Defizite der Normenklarheit

Darüber hinaus begegnet § 184b LVwG-E Bedenken im Hinblick auf die Anforderungen an Normenklarheit und Vorhersehbarkeit.

Dies gilt zunächst für das **Tatbestandsmerkmal der „Ergänzung eines vorhandenen Sachverhalts“**. Der Gesetzentwurf betont zwar wiederholt, dass die biometrische Echtzeit-Fernidentifizierung nicht anlasslos, sondern lediglich zur Ergänzung eines bereits bestehenden Sachverhalts zulässig sein soll.³⁰ Der Begriff wird jedoch weder im Gesetz noch in der Begründung hinreichend konkretisiert. Insbesondere bleibt offen, welchen Konkretisierungsgrad der zugrunde liegende Sachverhalt aufweisen muss und welche tatsächlichen Erkenntnisse bereits vorliegen müssen, bevor die Maßnahme eingeleitet werden darf. Dadurch wird der Anwendungsbereich der Befugnis nur eingeschränkt vorhersehbar.

Zweifel an der Normenklarheit ergeben sich zudem aus der gewählten **Verweisungstechnik**. Zwar gibt die KI-Verordnung den Rahmen für eine im nationalen Recht zu schaffende Rechtsgrundlage zum Einsatz eines KI-getriebenen biometrischen Echtzeit-Fernidentifizierungssystems vor (vgl. Art. 5 Abs. 5 S. 1 und 3 KI-VO).

²⁹ OHCHR, A/HRC/48/31: The right to privacy in the digital age (2021), S. 7.

³⁰ Drucksache 20/4284, S. 43f.



Der angestrebte Ausgleich zwischen unionsrechtlichem Normwiederholungsverbot³¹ und verfassungsrechtlichen Bestimmtheitsanforderungen gelingt jedoch kaum. So benennt § 184b LVwG-E einzelne Schutzgüter wie Leben, Leib, Freiheit oder die sexuelle Selbstbestimmung ausdrücklich selbst, verweist für deren genaue Reichweite jedoch zugleich auf die entsprechenden Regelungen der KI-Verordnung. Dadurch entsteht eine hybride Regelungstechnik aus eigenständiger landesrechtlicher Regelung und unionsrechtlicher Verweisung. Dies mag die Lesbarkeit nur punktuell verbessern und birgt die **Gefahr künftiger Auslegungsdifferenzen** zwischen dem unionsrechtlichen Regelungsgehalt und den landesrechtlichen Formulierungen. Aus Gründen der Normenklarheit wäre es vorzugswürdig, die zulässigen Einsatzzwecke und tatbestandlichen Voraussetzungen vollständig und verständlich im Landesrecht selbst zu normieren und lediglich hinsichtlich technischer, verfahrensrechtlicher und sonstiger unionsrechtlich vorgegebener Detailanforderungen auf die KI-Verordnung zu verweisen. Gerade bei einer Befugnis, die die automatisierte biometrische Identifizierung von Personen im öffentlichen Raum ermöglicht, sollten die wesentlichen Voraussetzungen des Grundrechtseingriffs unmittelbar aus dem Gesetz selbst erkennbar sein.

2.1.5. Unzureichende Schutzmechanismen

Positiv hervorzuheben ist, dass der Gesetzentwurf die biometrische Echtzeit-Fernidentifizierung im Vergleich zu anderen Befugnissen mit einer Reihe zusätzlicher Schutzmechanismen versieht. Hierzu zählen insbesondere die Verpflichtung zu einer ausdrücklichen Verhältnismäßigkeitsabwägung (§ 184b Abs. 1 S. 4 LVwG-E), die Beschränkung der Maßnahme auf das zeitlich, örtlich und personenbezogen unbedingt erforderliche Maß (§ 184b Abs. 2 LVwG-E), der grundsätzliche Richter*innenvorbehalt, die auf sieben Tage begrenzte Anordnungsdauer mit der Pflicht einer erneuten richterlichen Entscheidung für jede Verlängerung (§ 184b Abs. 3 LVwG-E) und die zweifache menschliche Überprüfung von “Treffern” des Systems (§ 184c Abs. 1 S. 2 LVwG-E). Gleichwohl darf auch hier das Risiko des **Automation Bias** (s. 1.2.2. und 2.1.2.) nicht übersehen werden.

Problematisch erscheint zudem die **Eilkompetenz** nach § 184b Abs. 3 S. 5 LVwG-E. Gerade bei einer Maßnahme, die die automatisierte Verarbeitung biometrischer Daten einer Vielzahl von Personen im öffentlichen Raum ermöglicht und damit zu den eingriffsintensivsten polizeilichen Befugnissen zählt, kommt dem Richter*innenvorbehalt eine zentrale grundrechtssichernde Funktion zu. Diese besteht gerade darin, eine unabhängige Kontrolle vor Beginn des Eingriffs sicherzustellen. Hinzu kommt, dass die Eilanordnung nicht ausschließlich den Leitungen des Landespolizeiamtes, des Landeskriminalamtes oder einer Polizeidirektion vorbehalten ist, sondern auch auf besonders beauftragte Personen des Polizeivollzugsdienstes übertragen werden kann.

Besonders problematisch ist überdies das mit der Maßnahme verbundene Transparenz- und Rechtsschutzdefizit. Während nach § 184c Abs. 2 LVwG-E **nur die Zielperson benachrichtigt wird, bleibt die Verarbeitung der biometrischen Daten aller übrigen im Erfassungsbereich befindlichen Personen regelmäßig folgenlos und unsichtbar**. Es ist nicht zu erwarten, dass Passant*innen bei Hinweisen auf Videoüberwachung auch eine Live-Gesichtserkennung annehmen, ein gesonderter Hinweis darauf ist - anders als beim Einsatz von Verhaltensscannern - jedoch nicht vorgesehen. Damit fehlt gerade dem größten Teil der von der Datenverarbeitung Betroffenen regelmäßig die tatsächliche Möglichkeit, gerichtlichen oder datenschutzrechtlichen Rechtsschutz in Anspruch zu nehmen. Dies wirft erhebliche Fragen hinsichtlich der Effektivität der Rechtsschutzgarantie aus Art. 19 Abs. 4 GG sowie des Anspruchs auf einen wirksamen Rechtsbehelf auf.

Schließlich ist zu begrüßen, dass der Entwurf die biometrische Echtzeit-Fernidentifizierung besonderen **Dokumentations-, Datenschutz- und Kontrollanforderungen** unterwirft. Nach § 184c Abs. 3 S. 2 LVwG-E sind

³¹ Drucksache 20/4284, S. 44, vgl. EuGH, Urt. v. 10. Oktober 1973, 34/73 = BeckRS 2004, 70873 Rn. 9 bis 11; Streinz/W. Schroeder, 3. Aufl. 2018, AEUV Art. 288 Rn. 43.



über die allgemeinen Protokollierungspflichten des § 186c LVwG hinaus auch die jeweils eingesetzte automatisierte Anwendung sowie die für die Durchführung verantwortliche Mitarbeiterin oder der verantwortliche Mitarbeiter zu dokumentieren. Zudem führt die Einbeziehung der §§ 184b, 184c LVwG-E in die Kontrollmechanismen der §§ 186b, 186c LVwG-E dazu, dass die Maßnahme den datenschutzrechtlichen Stichprobenkontrollen der oder des Landesbeauftragten für Datenschutz unterliegt und Gegenstand der Berichtspflicht gegenüber dem Landtag ist.

2.1.6. Fehlende Wirksamkeitsnachweise

Die biometrische Echtzeit-Fernidentifizierung ermöglicht einen der schwersten Grundrechtseingriffe des gesamten Gesetzentwurfs. Umso mehr überrascht, dass die Begründung nicht nachvollziehbar darlegt, weshalb die bereits bestehenden Instrumente der Gefahrenabwehr hierfür nicht ausreichen. Zwar werden mögliche Einsatzszenarien beschrieben, **ein belastbarer Nachweis eines konkreten zusätzlichen Sicherheitsgewinns bleibt jedoch weitgehend aus**. Insbesondere wird nicht aufgezeigt, in welchen Fällen herkömmliche Videoüberwachung, Fahndungsmaßnahmen oder Identitätsfeststellungen versagen und weshalb gerade die biometrische Echtzeit-Fernidentifizierung erforderlich sein soll.

Die **bisherige Praxis zeichnet vielmehr ein anderes Bild**: Obwohl automatisierte Gesichtserkennung und vergleichbare KI-gestützte Überwachungsinstrumente bereits in mehreren Bundesländern (Hessen, Hamburg und Baden-Württemberg) eingesetzt oder erprobt werden, **fehlen bislang belastbare Nachweise dafür, dass sie Straftaten verhindert oder in relevantem Umfang zur Aufklärung von Straftaten beigetragen hätten**.³²

2.2. NACHTRÄGLICHE FERNIDENTIFIZIERUNG, §§ 195B, 195C LVWG-E

Mit §§ 195b, 195c LVwG-E soll erstmals eine Rechtsgrundlage für die **biometrische Identifizierung von Personen anhand öffentlich zugänglicher Internetdaten** geschaffen werden. Die Vorschrift ermöglicht es der Polizei, biometrische Referenzdaten mit Bild- und Videomaterial aus öffentlich zugänglichen Online-Quellen automatisiert abzugleichen, um Personen zu identifizieren. Die Regelung ermöglicht damit eine systematische biometrische Durchsuchung öffentlich zugänglicher digitaler Räume und schafft eine neue Form datengetriebener Fahndung, die weit über herkömmliche Ermittlungs- und Identifizierungsmaßnahmen hinausgeht.

§ 195b LVwG-E gehört zu den eingriffsintensivsten Regelungen des Gesetzentwurfs. Die Kombination aus erheblicher Eingriffsintensität und Streubreite (s. 2.2.1.), Fehler-, Diskriminierungs- und Missbrauchsrisiken (s. 2.2.2.), Einschüchterungseffekten (s. 2.2.3.), Bestimmtheitsdefiziten und unionsrechtlichen Unsicherheiten (s. 2.2.4.) sowie unzureichenden Schutzmechanismen (s. 2.2.5.), begegnet schwerwiegenden grund- und menschenrechtlichen Bedenken. Die Regelung sollte daher nicht verabschiedet werden.

2.2.1. Erhebliche Eingriffsintensität

Die Maßnahme greift erheblich in das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG ein. Das Eingriffsgewicht ergibt sich nicht nur aus der Verarbeitung biometrischer Daten als besonders sensibler Kategorie personenbezogener Informationen. Darüber hinaus werden Bild-, Audio- und Videodateien automatisiert ausgewertet, um aus ihnen biometrische Merkmale zu extrahieren, in

³² <https://netzpolitik.org/2025/polizeigesetz-entwurf-auch-schleswig-holstein-will-verhaltensscanner/>.



durchsuchbare Referenzdaten zu verwandeln und für neue Identifizierungs- und Erkenntniszwecke nutzbar zu machen.

Besonders problematisch ist die außergewöhnliche **Streubreite** der Maßnahme. Anders als § 195 Abs. 2 LVwG-E beschränkt sich die Vorschrift nicht auf bereits vorhandene polizeiliche Datenbestände, sondern ermöglicht die automatisierte Durchsuchung öffentlich zugänglicher Internetquellen nach biometrischen Merkmalen. Erfasst werden damit potenziell die veröffentlichten Bild-, Audio- und Videodaten einer **unüberschaubaren Zahl von Personen**, von denen die überwiegende Mehrheit **weder Anlass für die Maßnahme gegeben hat noch in einem Zusammenhang mit der zugrunde liegenden Gefahrenlage** steht. Betroffen sind zudem regelmäßig Personen, die lediglich beiläufig auf Fotografien oder in Videoaufnahmen Dritter erscheinen.

2.2.2. Risiko von Fehlidentifikationen, Diskriminierung und Missbrauch

Hinsichtlich der Risiken von Fehlidentifikationen, diskriminierenden Auswirkungen und technischen Fehluordnungen kann auf die Ausführungen zu § 184b LVwG-E verwiesen werden (s. 2.1.2.).

Besondere Risiken ergeben sich bei § 195b LVwG-E jedoch aus der **Nutzung öffentlich zugänglicher Internetdaten**. Die herangezogenen Bild-, Audio- und Videodaten werden regelmäßig nicht zu Identifizierungszwecken erstellt oder erhoben. Ihre Qualität, Aktualität, Vollständigkeit und Eignung für biometrische Analysen können erheblich variieren. Hinzu kommt, dass Inhalte im Internet häufig aus ihrem ursprünglichen Kontext gelöst werden und ihre Herkunft oder Authentizität nicht stets verlässlich überprüfbar ist. Dies erhöht das Risiko fehlerhafter Zuordnungen und kann aufgrund der erheblichen Streubreite der Maßnahme zu einer ungerechtfertigten Einbeziehung unbeteiligter Personen in polizeiliche Ermittlungen führen.

Schließlich erhöht die Vorschrift auch die **Missbrauchsrisiken**. Anders als polizeiliche Datenbestände beruhen öffentlich zugängliche Internetquellen auf Inhalten, die durch Dritte gezielt im Internet veröffentlicht, verändert oder aus dem Zusammenhang gerissen werden können. Es besteht daher das Risiko, dass falsche Spuren gelegt, Ermittlungen beeinflusst oder Dritte zu Unrecht mit einer gesuchten Person in Verbindung gebracht werden. Die Vorschrift erweitert damit nicht nur die Möglichkeiten biometrischer Identifizierung, sondern auch die Gefahr fehlerhafter oder manipulativ herbeigeführter Zuordnungen.

2.2.3. Einschüchterungseffekte

Zudem birgt auch § 195b LVwG-E erhebliche Einschüchterungs- und Abschreckungseffekte (chilling effects). Die Aussicht, dass veröffentlichte Fotos, Videos oder Audiodateien nachträglich automatisiert analysiert und zur Identifizierung von Personen herangezogen werden können, ist geeignet, das Kommunikations- und Veröffentlichungsverhalten zu beeinträchtigen. Personen könnten etwa davon absehen, Inhalte mit Bezug zu politischen, gesellschaftlichen, religiösen oder kulturellen Aktivitäten zu veröffentlichen oder an öffentlichen Debatten teilzunehmen, wenn sie befürchten müssen, hierdurch später biometrisch identifizierbar zu werden.

Das Bundesverfassungsgericht hat hervorgehoben, dass die freie Entfaltung der Persönlichkeit voraussetzt, dass der Einzelne grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten bestimmen kann. Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen bekannt sind und wie diese verwendet werden, kann in seiner Freiheit wesentlich gehemmt werden.³³ Zwar müssen Nutzer*innen öffentlich zugänglicher Internetangebote damit rechnen, dass veröffentlichte Inhalte von Dritten eingesehen werden können. **Sie müssen jedoch nicht erwarten, dass diese**

³³ BVerfG, Urt. vom 15.12.1983, 1 BvR 209/83, BVerfGE 65, 1, Rn. 147.



Inhalte nachträglich automatisiert zu biometrischen Identifikatoren verarbeitet und für staatliche Identifizierungsmaßnahmen genutzt werden. Gerade diese Zweckverschiebung verstärkt das Risiko von Einschüchterungseffekten erheblich.

2.2.4. Defizite der Bestimmtheit und der Vereinbarkeit mit der KI-Verordnung

Außerdem bestehen erhebliche Bedenken bezüglich der **Bestimmtheit** des § 195b LVwG-E. Das Bundesverfassungsgericht hat sowohl im Volkszählungsurteil³⁴ als auch in seiner Entscheidung zur automatisierten Datenanalyse³⁵ hervorgehoben, dass die Zusammenführung, Auswertung und Generierung neuer personenbezogener Erkenntnisse durch technische Verfahren ein eigenständiges Eingriffsgewicht begründen kann und deshalb einer hinreichend bestimmten gesetzlichen Grundlage bedarf. Gerade bei neuartigen datenintensiven Überwachungsinstrumenten dürfen technische Möglichkeiten nicht an die Stelle normativer Begrenzungen treten. Vielmehr müssen **Herkunft, Rechtmäßigkeit, Umfang und Verwendungsgrenzen der zugrunde liegenden Datenbestände** gesetzlich hinreichend klar bestimmt und wirksam kontrollierbar sein.³⁶ Vor diesem Hintergrund bestehen erhebliche Zweifel, ob § 195b LVwG-E die Herkunft, technische Grundlage und rechtliche Zulässigkeit der für den biometrischen Abgleich erforderlichen Datenbestände mit der vom Bundesverfassungsgericht geforderten Bestimmtheit regelt. Die Vorschrift eröffnet weitreichende Identifizierungsmöglichkeiten, ohne die Voraussetzungen der hierfür erforderlichen Dateninfrastruktur selbst näher zu bestimmen.

Unklar bleibt zudem, wie die in § 195b LVwG-E vorgesehene biometrische Fernidentifizierung mit Art. 5 Abs. 1 lit. e KI-VO vereinbart werden soll. Die Vorschrift verbietet KI-Systeme zur Erstellung oder Erweiterung von Gesichtserkennungsdatenbanken durch ungezieltes Auslesen von Gesichtsbildern aus dem Internet oder aus Überwachungsaufnahmen. Erwägungsgrund 43 KI-VO verdeutlicht, dass das Verbot darauf abzielt zu verhindern, dass durch das ungezielte Auslesen von Gesichtsbildern aus dem Internet die **infrastrukturellen Voraussetzungen umfassender Identifizierbarkeit** geschaffen werden. Der Ordnungsgeber hebt hervor, dass hierdurch ein Gefühl ständiger Überwachung entstehen und die Grundrechte auf Privatheit und Datenschutz beeinträchtigt werden können.³⁷

Gerade diese Problematik stellt sich bei § 195b LVwG-E in besonderer Weise. Die Gewinnung der für den biometrischen Abgleich erforderlichen Vergleichsdaten aus dem Internet ist nicht lediglich vorgelagerte Voraussetzung der Maßnahme, sondern Teil des durch § 195b LVwG-E erlaubten Verarbeitungsvorgangs selbst. Nach *Teichmann* liegt die **rechtlich relevante Unterscheidung** weniger zwischen Echtzeit- und nachträglicher Identifizierung als vielmehr **zwischen geschlossenen, rechtmäßig aufgebauten Referenzbeständen und offenen Internetdatenräumen**. Für einen automatisierten biometrischen Identitätsabgleich genügt es nicht, einzelne Bilder im Internet aufzurufen und manuell zu vergleichen. Vielmehr muss das biometrische Referenzbild einer gesuchten Person technisch mit einer Vielzahl potenzieller Vergleichsbilder abgeglichen werden. Ein solcher automatisierter Abgleich einer Person mit zahlreichen gespeicherten Datensätzen ("One-to-Many-Abgleich") setzt nach gegenwärtigem technischen Stand strukturierte und durchsuchbare Gesichtsdatenbanken voraus. Besteht die technische Funktionsfähigkeit eines biometrischen Suchsystems faktisch nur auf Grundlage derartiger Datenbestände, entsteht ein Spannungsverhältnis zwischen der nach nationalem Recht eröffneten Befugnis und den unionsrechtlichen Grenzen für die hierfür erforderliche Dateninfrastruktur.

Die Gesetzesbegründung tritt diesem Einwand entgegen. Danach erfasse Art. 5 Abs. 1 lit. e KI-VO lediglich das ungezielte und vorratsmäßige Anlegen von Gesichtserkennungsdatenbanken, nicht jedoch die anlassbezogene Verarbeitung öffentlich zugänglicher Internetdaten. Die nach §§ 195b, 195c LVwG-E

³⁴ BVerfG, Urt. vom 15.12.1983, 1 BvR 209/83, BVerfGE 65, 1, Rn. 147f.

³⁵ BVerfG, Urt. vom 16.02.2023, 1 BvR 1547/19, BVerfGE 165, 363, Rn. 50, 67ff.

³⁶ BVerfG, Urt. vom 16.02.2023, 1 BvR 1547/19, BVerfGE 165, 363, Rn. 78ff.

³⁷ Art. 5 Abs. 1 lit. e KI-VO; Erwägungsgrund 43 KI-VO.



erhobenen Daten würden ausschließlich zweckgebunden für den konkreten Einzelfall verarbeitet, dürften nicht für zukünftige Verfahren vorgehalten werden und seien nach Abschluss des Abgleichs grundsätzlich unverzüglich zu löschen. Daher werde keine von Art. 5 Abs. 1 lit. e KI-VO erfasste Gesichtserkennungsdatenbank geschaffen.³⁸

Diese Argumentation beantwortet jedoch nicht die vorgelagerte Frage, auf welcher technischen Grundlage der von § 195b LVwG-E vorgesehene biometrische Abgleich praktisch erfolgen soll. Sowohl *Teichmann* als auch die Stellungnahme der Wissenschaftlichen Dienste des Deutschen Bundestages weisen darauf hin, dass ein automatisierter biometrischer Identitätsabgleich mit öffentlich zugänglichen Internetdaten **eine strukturierte und durchsuchbare Datenbasis, also eine vorratsmäßig angelegte Datenbank, voraussetzt**.³⁹ Die untersuchten Alternativen erwiesen sich demgegenüber entweder als technisch ungeeignet oder als praktisch nicht realisierbar.⁴⁰

2.2.5. Unzureichende Schutzmechanismen

Die Schutzarchitektur der §§ 195b, 195c LVwG-E orientiert sich weitgehend an den für die biometrische Echtzeit-Fernidentifizierung vorgesehenen Sicherungen. Die dort im Hinblick auf Richter*innenvorbehalt, Zweckbindungs- und Löschungsvorgaben, Benachrichtigungspflichten sowie Dokumentations- und Kontrollmechanismen geäußerten Bedenken gelten daher grundsätzlich auch hier (s. 2.1.5.).

3. Automatisierte Datenerhebung im öffentlichen Verkehrsraum, § 184d LVwG-E

Mit § 184d LVwG-E soll erstmals eine eigenständige Rechtsgrundlage für den **Einsatz automatisierter Bildauswertungssysteme im öffentlichen Verkehrsraum** geschaffen werden. Die Vorschrift ermächtigt die Polizei, Fahrzeuge und Fahrzeugführende offen zu erfassen, Kennzeichen sowie weitere Begleitdaten wie Ort, Zeit und Fahrtrichtung zu dokumentieren und die angefertigten **Bildaufzeichnungen automatisiert auf Muster auszuwerten, die auf die unerlaubte Nutzung elektronischer Geräte während der Fahrzeugführung hindeuten**. Ziel der Regelung ist die Verhütung sogenannter Ablenkungsverstöße nach § 23 Abs. 1a StVO. Nach der Gesetzesbegründung sollen rechtswidrig handelnde Fahrzeugführende „aus der Anonymität herausgehoben“ und hierdurch generalpräventive Verhaltenswirkungen erzielt werden.⁴¹

Die Befugnis stellt einen weiteren Schritt hin zu einer anlasslosen und automatisierten Verhaltensüberwachung im öffentlichen Raum dar. **Die Vorschrift verbindet eine erhebliche Eingriffsintensität mit einer niedrigen Eingriffsschwelle und einer weitreichenden Erfassung unbeteiligter Personen** (s. 3.1.). Die vorgesehenen Schutzmechanismen vermögen diese Grundrechtsrisiken nicht vollumfänglich aufzufangen, sodass erhebliche Zweifel an der Verhältnismäßigkeit der Regelung bestehen (s. 3.2.). Die Regelung sollte daher in ihrer jetzigen Form nicht verabschiedet werden. Zumindest sind der Anwendungsbereich erheblich einzugrenzen, die tatbestandlichen Voraussetzungen deutlich zu konkretisieren und die Kontroll- und Schutzvorkehrungen substantiell zu stärken.

³⁸ Drucksache 20/4284, S. 59.

³⁹ Teichmann, NJOZ 2026, 705, Rn. 15 ff., 38 ff.; Wissenschaftliche Dienste des Deutschen Bundestages/Fachbereich Europa, Biometrischer Abgleich mit Bildern aus dem Internet, PE 6 - 3000 - 074/25; WD 5 - 3000 - 105/25, S. 8 f., 9.

⁴⁰ Wissenschaftliche Dienste des Deutschen Bundestages/Fachbereich Europa, Biometrischer Abgleich mit Bildern aus dem Internet, PE 6 - 3000 - 074/25; WD 5 - 3000 - 105/25, S. 8.

⁴¹ Änderungsantrag, Umdruck 20/6786, S. 30, 31.



3.1. ERHEBLICHE EINGRIFFSINTENSITÄT UND NIEDRIGE EINGRIFFSSCHWELLE

Die in § 184d LVwG-E vorgesehene automatisierte Datenerhebung und Bildauswertung greift erheblich in das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG ein. Die Maßnahme beschränkt sich nicht auf die offene Anfertigung von Bildaufzeichnungen im öffentlichen Verkehrsraum. Vielmehr erlaubt sie die automatisierte Analyse von Bilddaten mit dem Ziel, vermeintlich regelwidriges Verhalten zu erkennen und bestimmte Verkehrsteilnehmende aus der Vielzahl der erfassten Personen herauszufiltern. Ergibt die automatisierte Auswertung einen Treffer, können die erhobenen Daten zur Identifizierung der betroffenen Person und zur Einleitung weiterer polizeilicher oder ordnungsrechtlicher Maßnahmen herangezogen werden.

Das besondere Eingriffsgewicht der Vorschrift resultiert zudem aus ihrer **erheblichen Streubreite**. Die Maßnahme richtet sich nicht gegen konkret auffällige Fahrzeugführende, sondern erfasst zunächst sämtliche Verkehrsteilnehmenden im überwachten Bereich.⁴²

Vor diesem Hintergrund erscheinen die **Eingriffsvoraussetzungen** der Norm **besonders niedrig**. Die Maßnahme knüpft weder an eine konkrete Gefahr noch an einen konkreten Verdacht oder sonstige tatsächliche Anhaltspunkte für einen individuellen Rechtsverstoß an. Vielmehr ermöglicht § 184d LVwG-E die Anfertigung und automatisierte Auswertung von Bildaufnahmen allein zur allgemeinen Verhütung von Ablenkungsverstößen im Straßenverkehr.

3.2. UNZUREICHENDE SCHUTZMECHANISMEN UND UNVERHÄLTNISMÄßIGKEIT

Positiv hervorzuheben ist, dass § 184d LVwG-E verschiedene Schutzvorkehrungen vorsieht. Hierzu zählen insbesondere die verpflichtende Überprüfung automatisierter Treffer durch qualifizierte Polizeibeschäftigte (§ 184d Abs. 2), die sofortige automatisierte Löschung aller Daten bei Nichttreffern (§ 184d Abs. 3), Dokumentations- und Datenschutzkontrollmechanismen (§ 184d Abs. 4 i.V.m. § 186c) sowie die Pflicht zur schriftlichen Anordnung der Maßnahme einschließlich der Festlegung von Umfang, Dauer und zugrunde liegenden Lageerkennnissen (§ 184d Abs. 5). Zudem verweist die Vorschrift beim Einsatz von Hochrisiko-KI-Systemen auf die Anforderungen der KI-Verordnung.

Diese Vorkehrungen vermögen die mit der Maßnahme verbundenen Grundrechtseingriffe jedoch nur eingeschränkt zu kompensieren.

Die **menschliche Überprüfung** setzt erst nach der automatisierten Analyse der Bilddaten ein und ist daher nicht geeignet, den vorausgehenden Grundrechtseingriff zu verhindern. Hinzu kommt, dass auch im Rahmen der menschlichen Kontrolle die Gefahr eines Automation Bias besteht (s. 1.2.2.). Gleiches gilt für die **Löschpflicht**: Sie setzt erst nach Erfassung, Auswertung und Bewertung der Daten ein. Der informationelle Eingriff ist zu diesem Zeitpunkt bereits erfolgt und wird durch die nachträgliche Löschung nicht ungeschehen gemacht.

Auch die **Offenheit** der Maßnahme bietet nur begrenzten Schutz. Zwar soll die Überwachung kenntlich gemacht werden. Ob entsprechende Hinweise unter den Bedingungen des fließenden Verkehrs tatsächlich wahrgenommen werden, erscheint jedoch zweifelhaft.

Auch die von der Begründung hervorgehobene Beschränkung auf einen grundsätzlich **stichprobenweisen Einsatz** überzeugt im Hinblick auf die Angemessenheit der Maßnahme nicht. Nach der Gesetzesbegründung bezieht sich die Stichprobe lediglich auf die Auswahl bestimmter Kontrollorte und Kontrollzeiträume.⁴³

⁴² Änderungsantrag, Umdruck 20/6786, S. 33.

⁴³ Änderungsantrag, Umdruck 20/6786, S. 33f.



Innerhalb dieser Kontrollfenster werden sämtliche erfassten Fahrzeugführenden automatisiert überprüft. Die Regelung begrenzt damit zwar die räumliche und zeitliche Reichweite der Maßnahme, nicht jedoch ihre Intensität gegenüber den Betroffenen.

Hinzu kommt, dass § 184d Abs. 1 S. 3 LVwG-E einen **über die Stichprobe hinausgehenden Einsatz** bereits dann zulässt, wenn dokumentierte polizeiliche Lageerkenntnisse dies „erforderlich erscheinen lassen“. Nach der Gesetzesbegründung können hierfür bereits eine erhöhte Zahl festgestellter Verstöße oder Erkenntnisse aus der Unfallstatistik genügen.⁴⁴ Konkrete Schwellenwerte oder sonstige objektivierte Kriterien enthält die Norm hingegen nicht. Dies wirft die Gefahr einer schrittweisen Ausweitung der Überwachung auf. Werden **hohe Verstoßzahlen** selbst zum maßgeblichen Argument für weitere Überwachung, kann die **Maßnahme ihre eigene Intensivierung rechtfertigen**. Je umfassender kontrolliert wird, desto mehr Verstöße werden sichtbar; je mehr Verstöße festgestellt werden, desto leichter lässt sich weiterer Überwachungsbedarf begründen. Die Norm enthält keine hinreichend bestimmten Begrenzungen, die einer solchen Dynamik wirksam entgegenwirken würden. Auch der Verweis auf **Unfallstatistiken** trägt die Ausweitung der Befugnis nur eingeschränkt. Aus einer erhöhten Unfallbelastung folgt nicht ohne Weiteres, dass Ablenkung durch elektronische Geräte die maßgebliche Ursache des Unfallgeschehens ist oder dass gerade die automatisierte Verhaltensüberwachung das geeignete Mittel zur Risikoreduzierung darstellt. Die Vorschrift erlaubt damit eine intensive Datenerhebung auf Grundlage allgemeiner Risikoannahmen, ohne dass zwischen den jeweils überwachten Personen und der angenommenen Gefahrenlage ein konkreter Zusammenhang bestehen muss.

4. Datenerhebungen mittels mobiler Sensorträgersysteme, § 185e LVwG-E

Mit § 185e LVwG-E soll zur Rechtssicherheit eine eigenständige Rechtsgrundlage für den Einsatz mobiler Sensorträgersysteme zur polizeilichen Datenerhebung geschaffen werden. Die Vorschrift ermöglicht den Einsatz technisch ausgestatteter mobiler Plattformen, insbesondere unbemannter Fluggeräte (Drohnen), zur Erhebung von Bild-, Ton- und sonstigen Sensordaten im Rahmen polizeilicher Aufgabenwahrnehmung. Anders als stationäre Überwachungseinrichtungen sind **mobile Sensorträgersysteme flexibel einsetzbar** und können **kurzfristig sowie ortsunabhängig** zur Beobachtung und Datenerhebung eingesetzt werden. Die Regelung erweitert damit nicht lediglich bestehende Überwachungsbefugnisse, sondern schafft eine **neue mobile Überwachungsinfrastruktur**, die polizeiliche Datenerhebungen räumlich und tatsächlich deutlich flexibilisiert.

Amnesty International lehnt den Einsatz von mobilen Sensorträgern nicht grundsätzlich ab, er muss jedoch menschenrechtskonform ausgestaltet werden. Die Nutzung mobiler Sensorträgersysteme ermöglicht eine flexible, ortsunabhängige und für Betroffene häufig nur eingeschränkt wahrnehmbare Überwachung und geht damit mit einer erheblichen Eingriffsintensität einher (s. 4.1.). Den erweiterten Überwachungsmöglichkeiten stehen jedoch nur begrenzte zusätzliche Schutz- und Kontrollmechanismen gegenüber (s. 4.2.). Die Regelung sollte daher in ihrer derzeitigen Fassung nicht verabschiedet werden. Zumindest bedarf es engerer Einsatzvoraussetzungen sowie spezifischer Kontroll-, Transparenz- und Dokumentationspflichten, die der besonderen Mobilität und Reichweite der eingesetzten Systeme Rechnung tragen.

⁴⁴ Änderungsantrag, Umdruck 20/6786, S. 34.



4.1. ERHEBLICHE EINGRIFFSINTENSITÄT

Zwar enthält § 185e LVwG-E keine eigenständige Ermächtigung zur Erhebung personenbezogener Daten. Die Vorschrift erlaubt jedoch personenbezogene Daten, deren Erhebung nach anderen Vorschriften zulässig ist, mittels mobiler Sensorträgersysteme zu erfassen. § 185e Abs. 1 S. 2 LVwG-E benennt die hierfür in Betracht kommenden Ermächtigungsgrundlagen abschließend, unter anderem § 184 Abs. 1 bis 5 in Nr. 1. (vgl. hierzu 1.). Die Vorschrift **erweitert** damit zwar nicht unmittelbar die materiellen Voraussetzungen der **Datenerhebung**, wohl aber die **technischen und tatsächlichen Möglichkeiten ihrer Durchführung**.

Die Datenerhebung mittels mobiler Sensorträgersysteme greift erheblich in das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) ein. Das besondere Eingriffsgewicht der Vorschrift liegt nicht allein in der Art der erhobenen Daten, sondern auch in der durch § 185e LVwG-E ermöglichten **Mobilisierung der Überwachungsinfrastruktur**. Durch die ausdrückliche Zulassung mobiler Sensorträgersysteme, insbesondere polizeilicher Drohnen, werden Datenerhebungen räumlich flexibilisiert und technisch erheblich erleichtert. Die Möglichkeit, Überwachungsmaßnahmen aus größerer Distanz, aus der Luft und über größere Flächen hinweg durchzuführen, erweitert den Kreis der potenziell Betroffenen und erhöht die Wahrscheinlichkeit, dass auch Personen erfasst werden, die keinerlei Anlass für die Maßnahme gegeben haben. Die Maßnahme weist somit eine **erhebliche Streubreite** auf.

Das Eingriffsgewicht beschränkt sich dabei nicht auf die Erhebung einzelner Daten. Die Erfassung von Bild-, Standort-, Bewegungs- und Verkehrsdaten kann die Grundlage für weitergehende **Erkenntnisse über Aufenthaltsorte, Bewegungsmuster, soziale Kontakte und persönliche Lebensgewohnheiten** schaffen. Mobile Sensorträgersysteme ermöglichen es damit, Informationen zu gewinnen, die über eine punktuelle Beobachtung deutlich hinausgehen und Rückschlüsse auf das Verhalten von Personen über einen längeren Zeitraum oder über größere räumliche Zusammenhänge hinweg zulassen.

Ferner verstärkt die Mobilisierung der Überwachungsinfrastruktur durch § 185e LVwG-E mögliche **Einschüchterungseffekte** und damit verbundene mittelbare Grundrechtseingriffe (vgl. 1.1.2.).

Schließlich ergibt sich die Eingriffsintensität des § 185e LVwG-E nicht allein aus der Datenerhebung mittels mobiler Sensorträgersysteme, sondern auch aus deren **Zusammenwirken** mit den neuen Befugnissen zur automatisierten Datenanalyse und Datenverknüpfung nach §§ 188c, 188d LVwG-E. Die erhobenen Bild-, Standort-, Bewegungs- und Sensordaten erweitern den Datenbestand für spätere Analyseprozesse und können mit weiteren Informationsbeständen zusammengeführt werden. Das eigentliche **Überwachungspotenzial** entsteht daher häufig erst durch die nachgelagerte Verknüpfung und Auswertung der Daten, die weitreichende Erkenntnisse über Bewegungsmuster, soziale Kontakte und Verhaltensweisen ermöglichen kann. § 185e LVwG-E schafft damit die Grundlage für eine zunehmend vernetzte und datengetriebene Überwachung, deren Eingriffsintensität über die einzelne Datenerhebung deutlich hinausgeht.

4.2. UNZUREICHENDE SCHUTZMECHANISMEN

Positiv hervorzuheben ist zunächst, dass § 185e Abs. 2 LVwG-E für offene Datenerhebungen nach § 184 Abs. 1 bis 5 LVwG-E ausdrücklich klarstellt, dass auch der Einsatz mobiler Sensorträgersysteme offen zu erfolgen hat. Nach der Gesetzesbegründung soll die Offenheit durch einen gesonderten Hinweis auf den Einsatz der Sensorträgersysteme, etwa durch Beschilderungen, besondere Kennzeichnungen der eingesetzten Drohnen oder der sie steuernden Personen, gewährleistet werden.⁴⁵

⁴⁵ Änderungsantrag, Umdruck 20/6786, S. 51.



Diese Schutzwirkung bleibt jedoch begrenzt. Zum einen enthält die Gesetzesbegründung **keine näheren Anforderungen an Art, Umfang oder Reichweite der Hinweise**. Ob Betroffene die Datenerhebung insbesondere im Falle einer Drohne **tatsächlich wahrnehmen** können, hängt damit maßgeblich von der konkreten Ausgestaltung im Einzelfall ab. Zum anderen kann auf den Hinweis nach der Gesetzesbegründung verzichtet werden, wenn seine Umsetzung aufgrund besonderer Umstände, insbesondere wegen besonderer **Dringlichkeit**, nicht möglich erscheint und der Verzicht angesichts der Gefahrenlage gerechtfertigt wird.⁴⁶ Die Offenheit der Maßnahme steht damit unter einem vergleichsweise **weiten Ausnahmeverbehalt**.

Hinzu kommt, dass die Offenheit lediglich die Wahrnehmbarkeit des Einsatzes mobiler Sensorträgersysteme betrifft, nicht jedoch die durch sie ermöglichten Formen der Datenerhebung. Auch bei gekennzeichneten Drohnen oder sonstigen mobilen Sensorträgern bleibt für Betroffene regelmäßig nicht erkennbar, welche Daten konkret erhoben, welche technischen Sensoren eingesetzt, welche Bereiche erfasst oder in welchem Umfang die gewonnenen Daten weiterverarbeitet werden. Die **Transparenz** bezieht sich damit primär auf das Vorhandensein des Systems, **nicht auf die Reichweite der Datenerhebung**.

Schließlich enthält § 185e LVwG-E keine eigenständigen **Kontroll- oder Schutzmechanismen**, die der besonderen Mobilität und Flexibilität der eingesetzten Systeme Rechnung tragen. Insbesondere unterfällt § 185e LVwG-E nicht den besonderen Kontroll- und Protokollierungsmechanismen der §§ 186 ff. LVwG-E. Es bestehen daher Zweifel, ob die vorgesehenen Transparenzvorkehrungen den besonderen Grundrechtsrisiken der Maßnahme hinreichend Rechnung tragen.

5. Automatisierte Datenanalyse, §§ 188c, 188d LVwG-E

Mit § 188c LVwG-E wird erstmals eine ausdrückliche Befugnis zur automatisierten Datenanalyse eingeführt. Die Vorschrift schafft ein **gestuftes System unterschiedlicher Analysebefugnisse**.⁴⁷ Während § 188c Abs. 3 LVwG-E die automatisierte Auswertung **bestimmter polizeilicher Datenbestände** ermöglicht, eröffnet § 188c Abs. 4 LVwG-E unter strengerer Voraussetzungen weitergehende Analysebefugnisse. Ergänzend erlaubt § 188c Abs. 5 LVwG-E die Einbeziehung **weiterer staatlicher und sonstiger Datenquellen**. Darüber hinaus sieht § 188c Abs. 7 LVwG-E die Erstellung von **Verhaltensprofilen** vor. Die Vorschrift differenziert damit zwischen verschiedenen Formen automatisierter Datenanalyse und knüpft hieran unterschiedliche verfahrensrechtliche Anforderungen.

Die §§ 188c, 188d LVwG-E begegnen erheblichen grund- und menschenrechtlichen Bedenken. Die Formen der automatisierten Datenanalyse eröffnen die Möglichkeit, umfangreiche Datenbestände aus unterschiedlichen Quellen zusammenzuführen, neue Erkenntnisse über Personen zu generieren und unter bestimmten Voraussetzungen Verhaltensprofile zu erstellen. Hierdurch entsteht ein eigenständiges und erhebliches Eingriffsgewicht, das durch die potenziell große Streubreite der Maßnahmen zusätzlich verstärkt wird (5.1.). Darüber hinaus bestehen erhebliche Risiken von Fehltreffern, Fehlbewertungen und diskriminierenden Effekten (5.2.). Schließlich sehen die Regelungen keine hinreichenden Schutzvorkehrungen vor, um diesen Gefahren wirksam zu begegnen (5.3.). Die Regelung sollte daher in ihrer jetzigen Form nicht verabschiedet werden.

5.1. ERHEBLICHE EINGRIFFSINTENSITÄT

Die automatisierte Datenanalyse nach § 188c LVwG-E greift **erheblich in das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG** ein. Anders als die bislang bestehenden

⁴⁶ Änderungsantrag, Umdruck 20/6786, S. 51.

⁴⁷ Von einer Stellungnahme zum IT-Abgleich aus § 188c Abs. 1 LVwG-E wird abgesehen.



Befugnisse zum Datenabgleich und zur Rasterfahndung dient sie nicht lediglich dem **Auffinden und Abgleichen bereits vorhandener Informationen**. Vielmehr ermöglicht sie die automatisierte Zusammenführung und Auswertung großer Datenbestände, um **neue Erkenntnisse über Personen, Beziehungen, Netzwerke und Zusammenhänge zu generieren**. Der Gesetzentwurf hebt selbst hervor, dass auf diese Weise Erkenntnisse gewonnen werden können, die selbst bei Zugang zu sämtlichen Datenbeständen von Menschen kaum erlangt werden könnten.⁴⁸

Das besondere Eingriffsgewicht der Vorschrift resultiert aus ihrem **erheblichen Erkenntnispotenzial**. Das Bundesverfassungsgericht hat hervorgehoben, dass automatisierte Datenanalysen ein **eigenständiges Eingriffsgewicht entfalten**, dessen Intensität insbesondere auch von Umfang und Aussagekraft der Analyse abhängt. Besonders schwer wiegt der Eingriff, wenn die eingesetzten Analyseverfahren die Erstellung von Bewegungs-, Verhaltens- oder Beziehungsprofilen ermöglichen.⁴⁹

Die Befugnis zur automatisierten Datenanalyse weist zudem eine **erhebliche Streubreite** auf. Nach § 188c Abs. 4 und 5 LVwG-E können neben umfangreichen polizeilichen Datenbeständen auch Daten aus öffentlichen Registern, weiteren Informationssystemen, Datenbeständen Dritter, einzelnen (im Umfang jedoch nicht weiter beschränkten) Datensätzen aus dem Internet sowie Verkehrsdaten aus Funkzellenabfragen in die Analyse einbezogen werden.⁵⁰ Je nach herangezogenem Datenbestand können demnach auch **Zeug*innen, Geschädigte, Hinweisgeber*innen, Kontaktpersonen** oder **sonstige unbeteiligte Dritte** (deren Daten etwa aus Asservaten, Funkzellendatenabfragen oder Internetquellen stammen) Gegenstand der Analyse werden, ohne selbst Anlass für polizeiliche Maßnahmen gegeben zu haben. Die Zusammenführung dieser heterogenen Datenbestände ermöglicht die gleichzeitige Auswertung von Informationen aus **unterschiedlichen Erhebungs- und Verwendungszusammenhängen**.

Das Bundesverfassungsgericht hat hervorgehoben, dass das Eingriffsgewicht automatisierter Datenanalysen auch davon abhängt, in welchem Umfang Personen betroffen sind, die dem relevanten Geschehen objektiv nicht zurechenbar sind und dadurch dem Risiko weiterer polizeilicher Maßnahmen ausgesetzt werden.⁵¹ Die erhebliche **Streubreite** der vorgesehenen Datenanalyse erhöht daher das Gewicht des Eingriffs in das Recht auf informationelle Selbstbestimmung zusätzlich. Die Möglichkeit, Daten aus unterschiedlichen Quellen in einer gemeinsamen Analyseumgebung auszuwerten, begründet die Gefahr einer **faktischen Zusammenführung bislang getrennter Informationsbestände**. Zwar enthält § 188d Abs. 5 LVwG-E Vorgaben zur Speicherdauer. Die Vorschrift erlaubt jedoch die Vorhaltung der zusammengeführten Datenbestände über den eigentlichen Analysevorgang hinaus, solange dies für den Zweck der Datenanalyse erforderlich ist.⁵²

Besonders eingriffsintensiv ist zudem die in § 188c Abs. 7 LVwG-E ausdrücklich vorgesehene Erstellung von **Verhaltensprofilen**. Die Befugnis beschränkt sich insoweit nicht auf die Verknüpfung einzelner Informationen, sondern ermöglicht die Verdichtung unterschiedlicher Erkenntnisse zu umfassenden Aussagen über eine Person, ihr Verhalten und ihre sozialen Beziehungen.

Schließlich erschwert die mit der Datenanalyse **verbundene Intransparenz** nicht nur die Kontrolle staatlichen Handelns, sondern kann zudem **abschreckende Wirkungen** auf die Wahrnehmung grundrechtlich geschützter Freiheiten entfalten (chilling effects). Für die Bevölkerung ist regelmäßig **nicht vorhersehbar**, welche rechtmäßigen Kontakte, Kommunikationsvorgänge oder sonstigen Verhaltensweisen später in automatisierte Analysen einfließen und zu verdachtserzeugenden „Treffern“ führen können. Dies kann insbesondere die Ausübung der Meinungs- und Versammlungsfreiheit beeinträchtigen.

⁴⁸ Drucksache 20/4284, S. 30

⁴⁹ BVerfG, Urt. v. 16.2.2023, 1 BvR 1547/19, BVerfGE 165, 363, Rn. 77.

⁵⁰ Drucksache 20/4284, S. 52.

⁵¹ BVerfG, Urt. v. 16.02.2023, 1 BvR 1547/19, BVerfGE 165, 363, Rn. 76f.

⁵² Drucksache 20/4284, S. 55.



5.2. RISIKO VON FEHLTREFFERN UND DISKRIMINIERUNG

Das Eingriffsgewicht der automatisierten Datenanalyse wird zusätzlich durch das Risiko fehlerhafter, verzerrter oder diskriminierender Ergebnisse erhöht (vgl. 1.2.2., 2.1.2. und 2.2.2.). Anders als bei der biometrischen Fernidentifizierung sieht der Gesetzentwurf keine ausdrückliche Verpflichtung vor, Analyseergebnisse vor ihrer weiteren Verwendung durch besonders qualifizierte Beschäftigte auf Plausibilität, Belastbarkeit und mögliche Fehlbewertungen zu überprüfen. Dies erhöht die Gefahr von **Automation Bias**: Algorithmisch erzeugten Ergebnissen kann eine erhöhte Objektivität und Verlässlichkeit zugeschrieben werden, obwohl sie lediglich Wahrscheinlichkeits- und Zusammenhangsannahmen abbilden.

Ferner untersagt § 188d Abs. 3 LVwG-E zwar Analyseverfahren, die unmittelbar an die in Art. 3 Abs. 3 GG genannten Merkmale anknüpfen. Hierdurch werden **Diskriminierungsrisiken** jedoch nicht beseitigt. Verzerrungen können bereits in den zugrunde liegenden **Datenbeständen** angelegt sein und durch die Analyse reproduziert oder verstärkt werden. Zudem entstehen diskriminierende Effekte häufig mittelbar über sogenannte **Proxymerkmale**, die zwar nicht unmittelbar an geschützte Merkmale anknüpfen, mit diesen aber tatsächlich korrelieren. Auch der Ausschluss selbstlernender Systeme ist zu begrüßen, vermag entsprechende Risiken jedoch lediglich zu begrenzen, nicht auszuschließen. Untersuchungen von Amnesty International haben wiederholt gezeigt, dass automatisierte Datenanalysen auch bei nicht selbstlernenden Systemen **diskriminierende Auswirkungen** entfalten können, insbesondere wenn bestehende Verzerrungen in Datenbeständen oder Entscheidungsstrukturen fortgeschrieben werden.⁵³

5.3. UNZUREICHENDE SCHUTZMECHANISMEN UND VERBLEIBENDE GEFAHREN

Positiv hervorzuheben ist, dass § 188c LVwG-E verschiedene Schutzvorkehrungen vorsieht, darunter auch solche, die in vergleichbaren Regelungen und Entwürfen auf Bundes- und Länderebene bisher fehlen. Hierzu zählen insbesondere das Verbot der Verwendung biometrischer Daten (§ 188c Abs. 6 Nr. 1 LVwG-E), das Verbot selbstlernender Systeme (§ 188c Abs. 6 Nr. 2 LVwG-E), das Verbot eines unmittelbaren automatisierten Internetabgleichs (§ 188c Abs. 6 Nr. 3 LVwG-E), das Verbot der Verwendung nicht gekennzeichneten Daten (§ 188d Abs. 1 LVwG-E), Vorgaben für die Einbindung der oder des Landesdatenschutzbeauftragten (§ 188d Abs. 7 LVwG-E) sowie ein Richter*innenvorbehalt für besonders eingriffsintensive Formen der Datenanalyse nach § 188c Abs. 8 S. 2 Nr. 2 LVwG-E. Positiv zu bewerten ist ferner, dass der Entwurf automatisierte Gefährlichkeitsprognosen und Formen des Predictive Policing ausdrücklich ausschließt.

Diese Schutzvorkehrungen vermögen die mit der automatisierten Datenanalyse verbundenen Grundrechtseingriffe jedoch nur eingeschränkt zu kompensieren.

Zwar sieht der Gesetzentwurf für Analysen unter Verwendung besonders umfassender Daten nach § 188c Abs. 4 einen **Richter*innenvorbehalt** vor (§ 188c Abs. 8 S. 2 Nr. 2 LVwG-E). Die Erstellung von Verhaltensprofilen unterliegt jedoch **keinem eigenständigen Schutzregime**. Der Entwurf erkennt zwar ihre besondere Eingriffsintensität selbst an, indem ihre Erstellung gesondert angeordnet werden muss (§ 188c Abs. 8 S. 3 LVwG-E). Gleichwohl richtet sich die Anordnungszuständigkeit allein nach der zugrundeliegenden Datenanalyse. Erfolgt diese nach § 188c Abs. 3 LVwG-E, kann auch die Erstellung eines Verhaltensprofils

⁵³ Exemplarisch: Amnesty International France: Discriminatory algorithm used by the social security agency must be stopped, 2024, online: <https://www.amnesty.org/en/latest/news/2024/10/france-discriminatory-algorithm-used-by-the-social-security-agency-must-be-stopped/>; Amnesty International UK, *Automated Racism: How Police Data and Algorithms Code Discrimination into Policing*, 2025, online: <https://media.amnesty.org.uk/documents/Automated20Racism20Report20-20Amnesty20International20UK20-202025.pdf>, Amnesty International, *Xenophobic machines: Discrimination through unregulated use of algorithms in the Dutch childcare benefits scandal*, 2021, online: <https://www.amnesty.org/en/documents/eur35/4686/2021/en/>.



aufgrund einer polizeilichen Anordnung erfolgen (§ 188c Abs. 8 S. 2 Nr. 1 LVwG-E). Angesichts der auch vom Bundesverfassungsgericht hervorgehobenen Eingriffsintensität von Verhaltens- und Beziehungsprofilen⁵⁴ genügt dies nicht.

Hinzu kommt, dass die Regelungstechnik des § 188c Abs. 8 LVwG-E sehr verschachtelt und schwer nachvollziehbar ist. Die Voraussetzungen und Zuständigkeiten für die Erstellung von Verhaltensprofilen erschließen sich erst aus einem komplexen Zusammenspiel verschiedener Absätze und Verweisungen. Dies begegnet mit Blick auf die **Normenklarheit** Bedenken. Die Unübersichtlichkeit der Regelung erscheint besonders problematisch, weil gerade die Ausgestaltung der Vorabkontrolle eine zentrale Schutzfunktion gegenüber den erheblichen Grundrechtseingriffen automatisierter Profilbildung erfüllt.

Auch das zu begrüßendes Verbot **selbstlernender Systeme** kann den zentralen Gefahren der automatisierten Datenanalyse nur teilweise begegnen. Bereits regelbasierte Analysesysteme können umfangreiche Datenbestände zusammenführen, neue Zusammenhänge sichtbar machen und umfassende Persönlichkeits-, Verhaltens- und Beziehungsprofile erstellen. Die den Analyseergebnissen zugrunde liegenden Verknüpfungen und Gewichtungen sind auch hier bereits **häufig nur eingeschränkt nachvollziehbar**. Dies erschwert die Kontrolle der gewonnenen Erkenntnisse und verstärkt die Gefahr intransparenter, faktisch kaum überprüfbarer Entscheidungsprozesse.

6. Ausweitung des Präventivgewahrsams, §§ 204, 205, 205a LVwG-E

Die Änderungen der §§ 204 ff. LVwG-E betreffen die **Voraussetzungen** und die **Dauer** des polizeilichen Präventivgewahrsams. Der Gesetzentwurf ergänzt die bereits bestehende Befugnis des § 204 Abs. 1 Nr. 2 LVwG zur Verhinderung unmittelbar bevorstehender Straftaten um **einen neuen Gewahrsamstatbestand in § 204 Abs. 1 Nr. 3 LVwG-E**. Danach soll eine Person künftig auch dann in Gewahrsam genommen werden können, wenn dies zur Abwehr einer Gefahr für Leben, Leib, Freiheit oder die sexuelle Selbstbestimmung einer Person unerlässlich ist. Zugleich wird mit § 204 Abs. 6 LVwG-E erstmals eine richterlich anzuordnende Gewahrsamsdauer von bis zu einem Monat mit Verlängerungsmöglichkeiten auf insgesamt **bis zu zwei Monaten** vorgesehen. Flankierend werden in § 205a LVwG-E neue verfahrensrechtliche Regelungen zum richterlichen Verfahren und zur anwaltlichen Vertretung geschaffen.

Diese Erweiterung begegnet erheblichen menschen- und verfassungsrechtlichen Bedenken. Die Novelle **senkt die Eingriffsschwelle** für den schwersten **präventiv-polizeilichen Grundrechtseingriff** deutlich ab (6.1.), erweitert die behördlichen **Prognosespielräume** (6.2.), wirft erhebliche Zweifel an der **Verhältnismäßigkeit** auf (6.3.) und sieht trotz einzelner Verbesserungen weiterhin keine **Schutzmechanismen** vor, die dem Gewicht des Eingriffs vollständig entsprechen (6.4.). Sie sollte nicht verabschiedet werden.

6.1. SCHWERSTE EINGRIFFSINTENSITÄT

Die Freiheitsentziehung stellt den schwersten Eingriff dar, den die Polizei **außerhalb des Strafverfahrens** gegenüber einer Person vornehmen kann. Sie betrifft unmittelbar das Grundrecht der Freiheit der Person aus Art. 2 Abs. 2 Satz 2 GG und unterliegt daher den besonderen Anforderungen des Art. 104 GG. Auch Art. 5 EMRK gewährleistet einen besonders strengen Schutz vor Freiheitsentziehungen.

⁵⁴ BVerfG, Urt. vom 16.02.2023, 1 BvR 1547/19, BVerfGE 165, 363. Rn. 73, 108.



Bereits nach bisherigem Recht konnte eine Person in Gewahrsam genommen werden, wenn dies unerlässlich war, um die unmittelbar bevorstehende Begehung oder Fortsetzung einer Straftat oder Ordnungswidrigkeit von erheblicher Bedeutung zu verhindern. Auch § 204 Abs. 1 Nr. 2 LVwG-E knüpft weiterhin nicht nur an Straftaten, sondern auch an **Ordnungswidrigkeiten** von erheblicher Bedeutung für die Allgemeinheit an, diese umfassen etwa nächtliche Ruhestörungen. Da bei präventivem Gewahrsam die strafprozessualen Schutz- und Verfahrensgarantien nicht zur Anwendung kommen, lehnt Amnesty International Formen administrativer Inhaftierung grundsätzlich ab. Eine polizeiliche Ingewahrsamnahme kann daher allenfalls zur Abwehr konkreter Gefahren im Zusammenhang mit Straftaten gerechtfertigt sein; die bloße Möglichkeit künftiger Ordnungswidrigkeiten genügt hierfür nicht.

Ferner entfällt beim neuen § 204 Abs. 1 Nr. 3 LVwG-E die bislang erforderliche **qualifizierte zeitliche Nähe des Schadenseintritts** ausdrücklich. Nach der Gesetzesbegründung soll künftig **bereits eine konkrete Gefahr genügen**; die Landesregierung beschreibt die Neuregelung selbst als eine Absenkung der Eingriffsschwelle gegenüber § 204 Abs. 1 Nr. 2 LVwG.⁵⁵ Damit wird der Anwendungsbereich des Präventivgewahrsams erheblich erweitert und die Entscheidung über eine Freiheitsentziehung in stärkerem Maße als bisher auf prognostische Bewertungen verlagert. Gerade bei Freiheitsentziehungen begegnet eine solche Vorverlagerung in das Gefahrenvorfeld besonderen **rechtsstaatlichen Bedenken**. Der Europäische Gerichtshof für Menschenrechte hat hervorgehoben, dass präventive Freiheitsentziehungen nur zulässig sind, wenn die zu verhindernde Handlung hinreichend konkret bestimmt werden kann und nicht lediglich eine allgemeine Gefährlichkeit der betroffenen Person angenommen wird.⁵⁶ Der Gerichtshof fordert insoweit eine enge Auslegung der Voraussetzungen des Art. 5 Abs. 1 lit. c EMRK.⁵⁷ Die Novelle verschiebt die Grenze zulässiger Freiheitsentziehungen deshalb deutlich **weiter in das Gefahrenvorfeld**, als dies nach bisherigem Landesrecht der Fall war.

6.2. ERWEITERTE PROGNOSEENTSCHEIDUNGEN UND UNBESTIMMTHEITSRISIKEN

Problematisch erscheint zudem die Art und Weise, wie die Neuregelung begründet wird. Zwar soll der neue Tatbestand auf Gefahren für besonders gewichtige Rechtsgüter beschränkt bleiben. Ob eine solche Gefahr vorliegt, hängt jedoch maßgeblich von Prognosen über das künftige Verhalten der betroffenen Person ab. Die Gesetzesbegründung stellt selbst klar, dass § 204 Abs. 1 Nr. 3 LVwG-E als **Auffangtatbestand** für Konstellationen dienen soll, in denen weder die Voraussetzungen des bisherigen Präventivgewahrsams noch diejenigen anderer Freiheitsentziehungen erfüllt sind.⁵⁸ Gerade dadurch entsteht jedoch ein besonders weiter Prognosespielraum und die Gefahr, dass die Grenze zwischen einer konkreten Gefahr und der bloßen Erwartung zukünftiger Rechtsgutverletzungen zunehmend verschwimmt. Je weiter die **Eingriffsschwelle in das Gefahrenvorfeld verlagert** wird, desto stärker hängt die Zulässigkeit der Freiheitsentziehung von wertenden Einschätzungen zukünftiger Entwicklungen ab. **Fehlprognosen wiegen hier besonders schwer**, weil sie unmittelbar den Entzug der persönlichen Freiheit zur Folge haben.

Hinzu kommt, dass der Gesetzentwurf die Prognoseentscheidung in § 204 Abs. 1 Nr. 2 LVwG-E durch sog. **legislative Prognosehilfen** konkretisiert. Fraglich erscheint jedoch, ob diese Kriterien den besonderen Anforderungen genügen, die an die Prognose einer Freiheitsentziehung zu stellen sind.

Dies gilt insbesondere für § 204 Abs. 1 Nr. 2 Buchst. b LVwG-E. Die Gesetzesbegründung versteht den Begriff der Waffe ausdrücklich weit und erfasst neben Waffen auch Werkzeuge sowie sonstige **Gegenstände**, die im Einzelfall als mögliche Angriffsmittel bewertet werden können.⁵⁹ Der Kreis relevanter Gegenstände

⁵⁵ Drucksache. 20/4284, S. 36, 72.

⁵⁶ EGMR, Urt. v. 22.10.2018, S., V. u. A./Dänemark, Nr. 35553/12, Rn. 89 ff.

⁵⁷ EGMR, Urt. v. 22.10.2018, S., V. u. A./Dänemark, Nr. 35553/12, Rn.89.

⁵⁸ Drucksache 20/4284, S. 35 f.

⁵⁹ Drucksache 20/4284, S. 71.



wird dadurch erheblich erweitert. Ob aus dem Mitführen eines solchen Gegenstands auf die unmittelbar bevorstehende Begehung einer Straftat geschlossen werden kann, bleibt dabei weitgehend polizeilichen Prognoseentscheidungen überlassen. Dies erscheint umso problematischer, als die Gesetzesbegründung selbst davon ausgeht, dass in vielen Fällen bereits die Sicherstellung des Gegenstands als milderes Mittel ausreichend sein kann.⁶⁰ Vor diesem Hintergrund bestehen Zweifel, ob die Vorschrift die Voraussetzungen einer Freiheitsentziehung hinreichend bestimmt begrenzt.

Auch die Prognosehilfe der **Wiederholungsgefahr** (§ 204 Abs. 1 Nr. 2 Buchst. c LVwG-E) begegnet Bedenken. Die Anknüpfung an frühere vergleichbare Vorfälle kann dazu führen, dass zurückliegendes Verhalten dauerhaft in künftige Gefahrenprognosen einfließt. Damit besteht die Gefahr, dass sich der Fokus polizeilicher Maßnahmen von der Verhinderung einer konkret drohenden Straftat zunehmend auf die Einschätzung der Person als potenziell gefährlich verlagert. Dies ist besonders problematisch, weil der Präventivgewahrsam nicht an vergangenes Fehlverhalten sanktionierend anknüpfen, sondern ausschließlich der Abwehr einer konkret bevorstehenden Gefahr dienen darf. Je stärker frühere Vorfälle die Gefahrenprognose prägen, desto größer wird das Risiko einer **fortdauernden Stigmatisierung** bereits polizeilich oder strafrechtlich in Erscheinung getretener Personen. Aus menschenrechtlicher Sicht ist dies besonders sensibel. Der EGMR hat in *S., V. und A. gegen Dänemark* betont, dass Art. 5 Abs. 1 lit. c EMRK keine generalpräventive Politik gegenüber als gefährlich angesehenen Personen zulässt, sondern lediglich die Verhinderung einer konkreten und spezifischen Straftat rechtfertigen kann. Die Behörden müssen Tatsachen vorweisen können, die einen objektiven Beobachter davon überzeugen würden, dass die betroffene Person mit hoher Wahrscheinlichkeit an einer solchen konkreten Straftat beteiligt gewesen wäre. Bloße Vermutungen oder allgemeine Gefährlichkeitsannahmen genügen hierfür nicht. Dies gilt umso mehr, als der Gesetzentwurf die Gefahrenprognose in erheblichem Umfang auf wertende Einschätzungen stützt, **ohne** hierfür **besondere Dokumentationsanforderungen** vorzusehen.

6.3. ZWEIFEL AN DER VERHÄLTNISSMÄßIGKEIT

Besonders kritisch erscheint die Verhältnismäßigkeit der Neuregelung.

Nach der ständigen Rechtsprechung des Bundesverfassungsgerichts setzt ein Eingriff in die Freiheit der Person voraus, dass kein gleich wirksames, die Betroffenen weniger belastendes Mittel zur Verfügung steht.⁶¹ Gerade vor diesem Hintergrund ist bemerkenswert, dass **derselbe Gesetzentwurf** die Möglichkeiten der elektronischen Aufenthaltsüberwachung nach § 201b LVwG-E erheblich erweitert.⁶² Denn die Landesregierung hebt selbst hervor, die elektronische Aufenthaltsüberwachung stelle gegenüber dem Präventivgewahrsam ein „**modernes milderes Mittel**“ dar und werde ausdrücklich gestärkt.⁶³ Gleichzeitig wird § 201b LVwG-E gerade mit dem Ziel ausgeweitet, Gefahren für Leib, Leben, Freiheit und sexuelle Selbstbestimmung bereits im Vorfeld überwachen und verhindern zu können.⁶⁴

Die Gesetzesbegründung verweist zwar darauf, dass Gewahrsam nur zulässig sein soll, wenn andere Mittel nicht ausreichen.⁶⁵ Sie legt jedoch nicht überzeugend dar, weshalb die gleichzeitig ausgeweitete elektronische Aufenthaltsüberwachung in den von § 204 Abs. 1 Nr. 3 LVwG-E erfassten Fallkonstellationen typischerweise nicht geeignet sein soll. Besonders deutlich wird dies mit Blick auf die **Schutzgüter**. Sowohl § 201b LVwG-E als auch § 204 Abs. 1 Nr. 3 LVwG-E dienen dem Schutz von Leib, Leben, Freiheit und sexueller Selbstbestimmung. Damit treffen zwei Instrumente aufeinander, die teilweise **dieselben Gefahrenlagen adressieren**, sich jedoch hinsichtlich ihrer Eingriffsintensität erheblich unterscheiden. Je

⁶⁰ ebd.

⁶¹ BVerfG, st. Rspr. zum Verhältnismäßigkeitsgrundsatz, etwa BVerfGE 141, 220; 65, 1.

⁶² Drucksache 20/4284, S. 37f.

⁶³ Drucksache 20/4284, S. 4 f., 38.

⁶⁴ Drucksache 20/4284, S. 63 f.

⁶⁵ Drucksache 20/4284, S. 72.



stärker der Gesetzgeber die elektronische Aufenthaltsüberwachung selbst als wirksames und milderes Mittel zur Abwehr solcher Gefahren ausbaut, desto höher sind die Anforderungen an die Begründung, weshalb in denselben Konstellationen ein vollständiger Freiheitsentzug erforderlich sein soll. Eine solche Begründung bleibt der Gesetzentwurf weitgehend schuldig.

6.4. UNZUREICHENDE SCHUTZMECHANISMEN

Positiv hervorzuheben ist, dass der Gesetzentwurf verschiedene rechtsstaatliche Sicherungen stärkt. Hierzu gehören insbesondere die ausdrückliche richterliche Entscheidung über die Fortdauer des Gewahrsams, die Einführung einer gesetzlichen Höchstdauer sowie die Bestellung anwaltlicher Vertretung von Amts wegen bei längerem Gewahrsam (§§ 204 Abs. 6, 205a LVWG-E).

Diese Verbesserungen vermögen die Erweiterung der Eingriffsbefugnisse jedoch nicht vollständig aufzufangen.

§ 204 Abs. 1 Nr. 1 LVWG-E sieht die Ingewahrsamnahme von Personen vor, wenn diese zu „ihrem Schutz gegen eine Gefahr für Leib oder Leben erforderlich ist, insbesondere, weil sie sich erkennbar in einem die freie Willensbestimmung ausschließenden Zustand oder sonst in hilfloser Lage befindet“. Die Gewährleistung der Handlungsfähigkeit und Autonomie von **Menschen mit psychischen Beeinträchtigungen** wird hierdurch nicht ausreichend berücksichtigt.⁶⁶

Besonders kritisch ist die Einführung einer möglichen **Gewahrsamsdauer von bis zu zwei Monaten**. Zwar betont die Gesetzesbegründung die Notwendigkeit richterlicher Einzelfallentscheidungen und verweist darauf, dass die Dauer des Gewahrsams verhältnismäßig festgelegt werden müsse.⁶⁷ Gleichwohl handelt es sich um einen außerordentlich langen präventiven Freiheitsentzug gegenüber Personen, die weder strafrechtlich verurteilt wurden noch Beschuldigte eines Strafverfahrens sein müssen. Die Eingriffsintensität nähert sich damit Bereichen an, die traditionell dem Strafprozessrecht vorbehalten sind.

Ferner setzt sich Amnesty International für eine **Videoüberwachung von Gewahrsamszellen** ein, da diese dazu beitragen kann, möglichem polizeilichen Fehlhandeln präventiv zu begegnen oder dieses zu dokumentieren. Aufnahmen können ebenso der Entlastung von Polizeibeamt*innen dienen, die zu Unrecht eines Übergriffs beschuldigt werden. § 205 Abs. 6 LVWG-E sollte daher nicht als Ermessensvorschrift gefasst werden. Neben dem im Entwurf vorgesehen Schutz der Intimsphäre muss auch das Recht auf vertrauliche Gespräche mit Rechtsbeiständen oder Ärzt*innen angemessen berücksichtigt werden. Es ist sicherzustellen, dass die Aufnahmen Beschwerdeführer*innen, Ermittler*innen und im Todesfall auch den Angehörigen zugänglich gemacht werden.

Insgesamt verschiebt die Novelle den Schwerpunkt des Präventivgewahrsams von der Verhinderung konkret bevorstehender Straftaten hin zu **prognosegestützten Freiheitsentziehungen im Gefahrenvorfeld**. Mit der Kombination aus abgesenkter Gefahrenschwelle, erweiterten Prognosespielräumen und einer möglichen Gewahrsamsdauer von bis zu zwei Monaten entsteht ein Instrument, das in erheblichem Umfang auf Annahmen über zukünftiges Verhalten gestützt wird. Dies entfernt sich deutlich von der Konstellation, die der EGMR in *S., V. und A. gegen Dänemark* als zulässige präventive Freiheitsentziehung angesehen hat (s. 6.1.). Die vorgesehene Regelung begegnet daher erheblichen Zweifeln im Hinblick auf Verhältnismäßigkeit, Freiheitsgrundrecht und die Anforderungen des Art. 5 EMRK.

⁶⁶ Vgl. zur allgemeinen Notwendigkeit der Desinstitutionalisierung: Ausschuss für die Rechte von Menschen mit Behinderung, Guidelines on deinstitutionalization, including in emergencies, CRPD/C/5, 2022, https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRPD/C/5.

⁶⁷ Drucksache 20/4284, S. 73 f.