

netzpolitik.org, e. V., Boyenstraße 41, 10115 Berlin

Per E-Mail
Schleswig-Holsteinischer Landtag
z. Hd. Jan Kürschner, Vorsitzender des Innen-
und Rechtsausschusses

Ansprechpartner:
Martin Schwarzbeck

martin.schwarzbeck@netzpolitik.org

Datum: 27.08.2026

Stellungnahme zum Gesetz zur Fortentwicklung polizeirechtlicher Maßnahmen für einen wirksamen Schutz der öffentlichen Sicherheit (Drucksache 20/4284)

Sehr geehrte Damen, Herren und Sternchen,
im Rahmen des schriftlichen Anhörungsverfahrens erging mit Schreiben vom 25. Juni 2026 seitens des Innen- und Rechtsausschusses des Schleswig-Holsteinischen Landtages die Bitte, meine Auffassung zum Gesetzentwurf (Drucksache 20/4284) darzulegen. Mit Schreiben vom 10. Juli wurde noch der Wunsch nachgereicht, auch zu dem Änderungsantrag von CDU und Bündnis 90/Die Grünen (Umdruck 20/6786) Stellung zu nehmen.

Angefragt wurde ich als Redakteur von netzpolitik.org. Dort habe ich zahlreiche Texte zum Polizeigesetz von Schleswig-Holstein und ähnlichen Vorhaben auf Landes- und Bundesebene veröffentlicht.

netzpolitik.org ist ein Medium für digitale Freiheitsrechte. Wir thematisieren die wichtigen Fragestellungen rund um Internet, Gesellschaft und Politik. Wir begleiten alle gesellschaftlichen Bereiche kritisch bei Prozessen der Digitalisierung: von den großen Datenkonzernen über die Sicherheitsbehörden bis hin zu Bildung, Medien und Umwelt. Wir wollen technologischen Wandel in den Dienst von Freiheit, Solidarität und Gemeinwohl stellen.

Ich bedanke mich vielmals für die Gelegenheit und übersende Ihnen im Folgenden meine Stellungnahme.

Mit freundlichen Grüßen

Martin Schwarzbeck
Redakteur netzpolitik.org

Einleitung

Aus Kapazitätsgründen konzentriert sich diese Stellungnahme auf die aus meiner Sicht problematischsten Befugnisse, als da wären:

§ 184 Datenerhebung bei öffentlichen Veranstaltungen und Ansammlungen sowie an allgemein zugänglichen Orten – dabei speziell die in Paragraf 5 beschriebene automatisierte Verhaltensanalyse und Nachverfolgung.

§ 184b (und c) Echtzeit-Fernidentifizierung in öffentlich zugänglichen Räumen.

§ 184d Automatisierte Datenerhebung im öffentlichen Verkehrsraum zur Erkennung von Ablenkungsverstößen.

§ 185 Besondere Mittel der Datenerhebung. Dort speziell die Erweiterung der Einsatzmöglichkeiten.

§ 188c (und d) IT-gestützter Abgleich; Datenanalyse.

§ 195b (und c) Nachträgliche Fernidentifizierung.

Für viele dieser Technologien sollen personenbezogene Daten verarbeitet werden – und zwar nicht nur die von Verdächtigen, sondern die aller Menschen an einem bestimmten Ort oder gar aller Menschen, zu denen Daten im Internet zu finden sind. Damit ist die Streubreite so hoch, dass sich die Maßnahmen nicht mit dem demokratischen Rahmen vertragen, in dem sie errichtet werden sollen. Sie schaffen eine Vorverdächtigung ohne Anhaltspunkt.

Die Maßnahmen sind einzeln und erst Recht in ihrer Gesamtheit enorm eingriffsintensiv und lassen in der Ausgestaltung eine fehlende Verhältnismäßigkeitsprüfung erkennen.

Die Nutzung von sogenannter Künstlicher Intelligenz ist im polizeilichen Kontext grundsätzlich abzulehnen. Hoheitliches Handeln sollte im demokratischen Kontext stets nachvollziehbar bleiben. Das ist mit derartigen Systemen aber nicht per se gegeben. Hier sind meist nur In- und Output für Menschen einsehbar, was dazwischen passiert, bleibt undurchsichtig.¹

Problematisch ist in dem Kontext auch der „Automation Bias“. Dieses verhaltenspsychologisch nachgewiesene Phänomen führt dazu, dass sich Menschen in ihren Entscheidungen ungebührlich stark auf die Vorschläge und Entscheidungen von Maschinen verlassen.² So werden diese im Zweifelsfall eben nicht kritisch hinterfragt, sondern regelmäßig einfach abgenickt. Dies trifft sicherlich umso stärker zu, als viele der von Menschen zu bestätigenden Entscheidungen im polizeilichen Kontext unter Zeitdruck getroffen werden müssen.

Mit der Überwachung durch ein automatisiertes System gehen insbesondere aufgrund der Nicht-Nachvollziehbarkeit und beinahe-selbstverständlichen Entscheidungsübernahme erhebliche Einschüchterungseffekte für die betroffenen Personen einher.³ Dies ist noch einmal problematischer angesichts der Tatsache, dass die Betroffenen der Maßnahmen im Rahmen einiger dieser Befugnisse keinerlei Kenntnis über ihre Betroffenheit haben und auch nicht nachträglich informiert werden sollen. Es bleibt Bürger*innen nur die Grundannahme, theoretisch zu jeder Zeit Objekt einer derartigen Überwachungstechnologie sein zu können.

1 <https://www.gsb.stanford.edu/insights/explainer-black-box-problem>

2 https://en.wikipedia.org/wiki/Automation_bias

3 <https://www.amnesty.de/informieren/blog/deutschland-wie-ueberwachung-die-meinungsfreiheit-gefaehrdet>

Zudem sind die Befugnisse nicht isoliert zu betrachten. Sie fügen sich ein in eine bereits jetzt beachtliche Überwachungsinfrastruktur in Bund und Land und erhöhen im Zusammenspiel ihre Eingriffstiefe noch einmal massiv– wenn etwa beispielsweise eine Person, die sich verdächtig verhält, aus der Ferne identifiziert und mit ihrem Bewegungs- und Kontaktprofil in eine polizeiliche Datenbank aufgenommen wird – was in der Gesamtschau der Befugnisse mit diesen theoretisch möglich ist.

Nicht zuletzt sollte bei der Ausweitung von Überwachungsbefugnissen immer auch mitgedacht werden, wie diese missbraucht werden könnten. Werkzeuge, wie sie der Entwurf einführen will, wären in der Hand autoritärer Kräfte ein Kickstart in einen totalitären Überwachungsapparat. Vernunft und Gewissen sollten die Zustimmung zu derartigen Befugnissen – speziell zu diesem Zeitpunkt der deutschen Geschichte – eigentlich verunmöglichen.

Traditionell werden Überwachungsbefugnisse mit der Zeit immer weiter ausgebaut. Die eine Schwelle, zu der es möglich ist, sie wirklich zu begrenzen, ist jetzt – vor ihrer Einführung.

§ 184 Datenerhebung bei öffentlichen Veranstaltungen und Ansammlungen sowie an allgemein zugänglichen Orten – dabei speziell die in Paragraph 5 beschriebene automatisierte Verhaltensanalyse und Nachverfolgung.

Die Befugnis soll ermöglichen, Videoüberwachung des öffentlichen Raums mit Software aufzurüsten, die erkennt, was Menschen tun und bei bestimmten Verhaltensweisen Alarm schlägt. Im Alarmfall soll eine weitere Software verdächtige Personen kennzeichnen und im Videoüberwachungsnetzwerk automatisiert nachverfolgen.

Die Technologie wird in Mannheim und Hamburg bereits eingesetzt und von ihren Vertreter*innen als besonders datenschutzfreundlich beworben, weil sie die Videoaufnahmen zu einer Art Strichmännchen-Cartoons reduziere.⁴ Tatsächlich ist es aber einfach eine weitere Ebene von Grundrechtseingriff, die zu der Videoüberwachung hinzukommt.⁵ In den Städten, in denen die Technologie bereits betrieben wird, schauen auch weiterhin Polizist*innen auf die Bildschirme. Spätestens bei Alarmierung bekommen diese den originalen Videostream angezeigt.

Die Umsetzung von Bewegungen in Vektoren erlaube angeblich eine weitreichende Anonymisierung und verhindere Diskriminierung, weil körperliche Merkmale wie Alter, Geschlecht oder Hautfarbe in die Auswertung der bewegten Vektorenbündel nicht einfließen würden, so Befürworter der Technologie. Tatsächlich ist aber das Bewegungsmuster eine höchstpersönliche Eigenschaft, die eine Identifikation (beispielsweise über Ganganalyse) problemlos ermöglicht.⁶

Das System soll Bewegungen erkennen, „die auf Handlungen hindeuten, mit welchen Leben, Leib, Freiheit oder die sexuelle Selbstbestimmung einer Person beeinträchtigt werden.“ Damit werden die gesuchten Verhaltensweisen nur äußerst vage definiert. Wonach konkret gesucht wird, würde damit auf untergesetzlicher Ebene ausgestaltet. Das erlaubt weite Gestaltungsspielräume, womöglich über die Intention des Gesetzgebers hinaus.

Möglich ist damit beispielsweise auch die automatische Erkennung liegender Personen, da diese ja Opfer einer Straftat geworden sein könnten. Eine derartig fokussierte Analyse würde aber obdachlose Personen diskriminieren.

Insbesondere problematisch ist die vage Definition wohl angesichts der angestrebten automatisierten Erkennung von Straftaten gegen die sexuelle Selbstbestimmung. Da der (fehlende) Konsens einer Berührung für eine Videokamera nicht ersichtlich ist, könnte damit jeglicher Körperkontakt zu einer Alarmierung führen.

Vorgeschrieben ist in dem Paragraphen, dass die Datenerhebung offen geschieht. In Mannheim und Hamburg wird mit Schildern darauf hingewiesen, die nach Größe und Anzahl offensichtlich ungenügend sind, um die Betroffenen über den Grundrechtseingriff zu informieren. Bei einer Umfrage in Mannheim⁷ beispielsweise war sich der Großteil der Befragten im überwachten Gebiet nicht bewusst, dass sie gerade

4 <https://www.iosb.fraunhofer.de/de/projekte-produkte/intelligente-videoueberwachung.html>

5 u.a. <https://www.landtag.ltsch.de/infothek/wahl20/umdrucke/06800/umdruck-20-06829.pdf>

6 <https://netzpolitik.org/2025/biometrische-gangerkennung-zeige-mir-wie-du-gehst-und-ich-sage-dir-wer-du-bist/>

7 <https://netzpolitik.org/2025/verhaltensscanner-im-mannheim-hier-wird-die-ueberwachung-getestet-die-so-viele-staedte-wollen/>

gefilmt werden und ihr Verhalten automatisiert ausgewertet wird. Die Vorschrift zur offenen Datenerhebung entschärft demnach den Paragraphen kaum.

Zu beachten ist, dass die Maßnahme zu einem Normierungsdruck von Verhalten führt, der über den von regulärer Videoüberwachung hinausweist. Wer weiß, dass sein Verhalten gerade kategorisiert wird (die Software erkennt ja zumindest in Mannheim und Hamburg nicht nur alarmierungsträchtiges Verhalten sondern zum Beispiel auch Verhaltensklassen wie „Tanzen“ oder „sich Umarmen“), wird sich womöglich eingeschränkter ausdrücken.

Betroffen sind alle Menschen, die sich im Überwachungsbereich aufhalten. Sie werden gefilmt, was schon ein Eingriff in ihr Recht auf informationelle Selbstbestimmung ist, darüber hinaus sollen die Aufnahmen auch noch sehr lange (mindestens einen Monat) gespeichert – und dann auch noch algorithmisch analysiert werden. Die Videoüberwachung dokumentiert damit nicht mehr nur, sondern bewertet das Verhalten von Menschen und verdächtigt sie selbstständig.

Hinsichtlich der gebotenen Verhältnismäßigkeitsprüfung ist insbesondere auch die Wirksamkeit der Maßnahme zu betrachten. Diese wurde allerdings noch nie unabhängig evaluiert und in Mannheim, wo die Technologie seit acht Jahren läuft, kann die Polizei bis heute keinen einzigen Fall nennen, in dem mit Hilfe der Verhaltenserkennung eine Straftat verhindert oder aufgeklärt worden wäre. Die Erforderlichkeit der Befugnis ist dementsprechend nicht belegt.

Die Technologie wird von ihren Befürworter*innen vor allem auch deshalb angestrebt, weil sie Effizienzgewinne biete. Die Polizei müsse damit weniger Personal in die Videoüberwachung investieren. Gerade diese Möglichkeit ist aber äußerst kritisch zu sehen, weil sie damit einen Fehlanreiz zur räumlichen Ausweitung der Überwachung setzt.

Dabei sind der Ausweitung der Videoüberwachung durch den Entwurf nur wenig Grenzen gesetzt. Sie soll demnach auch schon dann möglich sein, wenn Tatsachen die Annahme rechtfertigen, dass an einem Ort erhebliche Ordnungswidrigkeiten begangen werden. Damit ist für die Überwachung eines Ortes nicht, wie in vielen anderen Bundesländern, eine erhöhte Belastung mit Straftaten erforderlich, sondern es reicht schon die Annahme einer einzelnen künftigen erheblichen Ordnungswidrigkeit, also beispielsweise eine drohende unerlaubte Abfallentsorgung.

Die geplante Möglichkeit zur automatisierten Nachverfolgung über das Videoüberwachungsnetzwerk hinweg bringt dabei weitere grundrechtsrelevante Implikationen mit sich. Denn mit dieser ließen sich nicht nur Bewegungs- sondern über den Besuch bestimmter Lokalitäten oder dem Treffen anderer Menschen auch annähernde Persönlichkeitsprofile erstellen. Das gilt umso mehr, als die Befugnis im Entwurf zeitlich nicht beschränkt ist und räumlich mit dem Ausbau der Videoüberwachung zunehmend erweitert wird.

In Folge dieser Ausführungen empfehle ich, die Befugnis ersatzlos aus dem Entwurf zu streichen.

§ 184b (und c) Echtzeit-Fernidentifizierung in öffentlich zugänglichen Räumen.

Diese Befugnis soll ermöglichen, Videoüberwachung des öffentlichen Raums mit einer Software aufzurüsten, die automatisiert die Gesichter aller Menschen im Überwachungsbereich vermisst und mit einer Liste von gesuchten Gesichtern vergleicht.

Die Technologie wird bereits in Frankfurt am Main eingesetzt. Sie läuft dort seit Juli 2025. Der Nutzen ist dabei bislang nur anekdotisch belegt: Eine gesuchte Person wurde damit identifiziert. Hingegen führt der Überwachungsdruck dazu, dass Menschen das überwachte Areal nicht oder nur unter Unwohlsein begehen.⁸ Die Verhältnismäßigkeit der Befugnis ist insofern höchst fraglich.

Nach der JI-Richtlinie der EU⁹ ist die Verarbeitung von biometrischen Daten zudem nur dann erlaubt, wenn sie unbedingt erforderlich ist. Eine derartige Erforderlichkeit ist angesichts der hier geplanten Massenhaftigkeit der Gesichteranalyse kaum vorstellbar.

Besonders kritisch zu sehen ist der gleichzeitige Einsatz der Fernidentifizierung und der Verhaltenserkennung. In dem Moment, wo neben dem abstrahierten Verhalten auch das konkrete Gesicht einer Person analysiert ist, verliert die Verhaltenserkennung den angeblichen Privatsphärevorteil komplett.

Ich empfehle deshalb, die Befugnis ersatzlos aus dem Entwurf zu streichen.

8 <https://netzpolitik.org/2026/rotlichtviertel-frankfurt-am-main-hier-analysiert-die-polizei-jedes-gesicht/>

9 <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016L0680>

§ 184d Automatisierte Datenerhebung im öffentlichen Verkehrsraum zur Erkennung von Ablenkungsverstößen.

Diese Befugnis soll es ermöglichen, im Straßenraum Kameras zu betreiben, die mit einer Software verknüpft sind, die automatisiert Menschen aufspürt, die während der Fahrt technische Geräte bei deren Nutzung in der Hand halten (sogenannte Handysünder).

Dabei ist höchst zweifelhaft, ob diese Maßnahme erforderlich ist. Im Gesetzentwurf ist zwar die Rede davon, dass Handysünder Unfälle verursachen würden und deshalb mit dieser Art der automatisierten Verhaltensanalyse Leben gerettet werden könnten, Zahlen zu Unfällen wegen Ablenkung durch Elektronikgebrauch nennt der Entwurf aber nicht.

Zudem verliert er völlig die technische Entwicklung aus dem Blick. Die allermeisten Kfz-Halter*innen haben inzwischen Freisprechanlagen in ihren Gefährten, viele nutzen bereits Sprachsteuerung. Der „Handysünder“ dürfte damit ein Auslaufmodell sein, für das es keiner gesetzlichen Regelung bedarf und ganz sicher keine, die derart invasiv in die Grundrechte unzähliger Menschen eingreift, die nicht einmal im Verdacht stehen, gegen die Norm zu verstoßen.

Die Möglichkeit, derartige Verhaltenserkennung über Stichproben hinaus, also dauerhaft und flächendeckend, einzusetzen, „wenn dies aufgrund dokumentierter polizeilicher Lageerkenntnisse erforderlich erscheint“ verstößt zudem gegen die vom Bundesverfassungsgericht geforderte Einhegung von Überwachungsmaßnahmen.¹⁰

Ich empfehle, die Befugnis ersatzlos aus dem Entwurf zu streichen.

¹⁰ https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2010/03/rs20100302_1bvr025608.html

§ 185 Besondere Mittel der Datenerhebung. Dort vor allem die Erweiterung der Einsatzmöglichkeiten.

Die Befugnis soll den Einsatz heimlicher, auch längerfristiger Überwachung mittels Standortdaten, Videos und Audioaufnahmen auch gegen Menschen erlauben, die mutmaßlich eine Gefahr für „wesentliche Infrastruktureinrichtungen oder Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen“ darstellen.

Die wesentliche Infrastruktureinrichtung und die Anlage mit unmittelbarer Bedeutung für das Gemeinwesen sind Konzeptionen maximaler Dehnbarkeit, die letztlich jegliche Infrastruktureinrichtung beinhalten könnten. Zu befürchten ist, dass hier eine „Lex Letzte Generation“ geschaffen werden soll, die es ermöglicht, mit verdeckter Observation beispielsweise auch gegen Menschen vorzugehen, die planen, aus Protest Straßen zu besetzen.

Ich empfehle, die Erweiterung der Einsatzmöglichkeiten der heimlichen, auch längerfristigen Überwachung ersatzlos aus dem Entwurf zu streichen.

§ 188c (und d) IT-gestützter Abgleich; Datenanalyse.

Diese Befugnis soll es ermöglichen, Daten aus verschiedenen Quellen in einer Meta-Datenbank vorzuhalten und diese von sogenannter Künstlicher Intelligenz auswerten zu lassen.

Das widerspricht nicht nur dem verfassungsgerichtlichen Verbot von unbeschränkter Vorratsdatenspeicherung¹¹, sondern auch der Zweckbindung, der polizeilich erhobene Daten unterliegen. Womöglich könnte die Befugnis sogar den Aufbau einer deutschlandweiten Polizeidatenbank (P20) torpedieren, da eben die dort verfügbaren Daten durch die Polizei von Schleswig-Holstein der Zweckbindung entrissen werden könnten.

Dem Gesetzentwurf zufolge könnten in die Analyse-Datenbank nicht nur Informationen über verdächtige Personen, sondern auch Daten von beispielsweise Zeug*innen oder Anzeigen-Stellenden gespeichert werden. Einbeziehbar sind auch weitere Register, beispielsweise zu Kfz-Halter*innen, sowie Daten aus Asservaten, also beispielsweise beschlagnahmten Mobiltelefonen, wo über Fotos, Chats oder Kontaktlisten zahlreiche weitere Unbescholtene in die Analyse einbezogen würden. Es droht der Aufbau einer polizeilichen Datenbank, die all diese zuvor fragmentierten Daten vereint.

Big-Data-Analyse ist totalitär, weil sie alles mit allem verknüpfen will. Weil sie Menschen so durchsichtig machen soll wie möglich. Sie passt nur zu totalitären Systemen und bringt Staaten, die sie einsetzen, an den Rand dazu, wie gerade in den USA zu sehen ist.¹² Nicht zu unterschätzen ist das Missbrauchspotenzial. Bereits jetzt nutzen einzelne Polizisten Datenbanken, um Menschen zu stalken¹³. Der ihnen mögliche Eingriff in fremde Persönlichkeitsrechte würde mit der Big-Data-Analyse potenziert. Auch ein Missbrauch auf staatlicher Ebene ist nicht auszuschließen: wer seine Bürger*innen derart umfassend in den Blick nehmen kann, der wird diese Macht womöglich auch zunehmend nutzen.

Dabei greift die Befugnis in das Recht auf informationelle Selbstbestimmung aller Menschen ein, deren Daten für die Datenanalyse genutzt werden, die Streubreite ist also massiv. Dass die Analyse für die Betroffenen heimlich abläuft, macht für diese einen effektiven Rechtsschutz unmöglich.

Mit derartiger Technologie lassen sich auf Knopfdruck Listen von Verdächtigen erstellen. Die Funktionslogik der Systeme bleibt dabei naturgemäß im Dunkeln. Warum die KI was entscheidet ist eine Black Box. Und auch hier gibt es keinerlei Evaluation oder Daten, anhand derer sich eine Aussage über den tatsächlichen praktischen Nutzen der Technologie für die Polizei treffen lässt.

Ich empfehle dementsprechend, die Befugnis ersatzlos aus dem Entwurf zu streichen.

11 https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2010/03/rs20100302_1bvr025608.html

12 <https://netzpolitik.org/2026/us-einwanderungsbehoerde-mit-palantir-und-paragon-auf-migrantenjagd/>

13 Beispielhaft: <https://www.berliner-zeitung.de/article/stalking-berliner-polizist-besorgte-sich-illegal-daten-von-frauen-215680> Oder in den USA: <https://www.washingtonpost.com/technology/2026/08/19/we-found-cops-who-misused-flock-their-police-departments-didnt-know/>

§ 195b (und c) Nachträgliche Fernidentifizierung.

Diese Befugnis soll es ermöglichen, im Internet nach Gesichtern, Stimmen oder anderen biometrischen Merkmalen bestimmter Menschen zu suchen, um diese zu identifizieren und/oder weitere Informationen über sie zu erlangen.

Mit Hilfe dieser Technologie ließen sich, je nachdem, was ein Mensch so im Netz teilt, oder auf wie vielen Veranstaltungsfotos fremder Personen er beispielsweise zu finden ist, Bewegungsmuster und auch Beziehungsgeflechte offenlegen. Die Eingriffstiefe ist dabei kaum zu überschauen. Die Befugnis schließt beispielsweise nicht aus, dass auch besonders sensible Daten analysiert werden, wie Bilder von Demonstrationen, queeren Partys oder Gottesdiensten. Das Eingriffsgewicht ist aufgrund der Heimlichkeit der Maßnahme besonders hoch.

Der mutmaßliche Nutzen der Technologie ist auch hier nur anekdotisch belegt. Eine ehemalige RAF-Terroristin wurde damit aufgestöbert.

Dagegen hat die Befugnis eine enorme Streubreite. Denn um bestimmte Menschen im Internet zu finden, müssen biometrische Daten von weit mehr Menschen erfasst, analysiert und abgeglichen werden. Betroffen sind potenziell die Grundrechte aller Menschen, von denen es biometrische Daten im Internet gibt. Desweiteren ist zu beachten, dass damit wohl auch Bilder von Minderjährigen der Analyse unterzogen werden würden.

Die Verwendung biometrischer Daten ist immer ein Eingriff in die informationelle Selbstbestimmung¹⁴, zudem kann hier das Recht auf freie Meinungsäußerung berührt sein. Dass die Analyse für die Betroffenen heimlich abläuft, macht einen effektiven Rechtsschutz unmöglich.

Dass für die nachträgliche Fernidentifizierung nur „öffentlich zugängliche Daten“ genutzt werden sollen, verringert die Eingriffstiefe nicht ausreichend. Selbst wenn die betroffenen Personen die Bilder oder beispielsweise Podcasts selbst ins Netz gestellt haben sollten, dann haben sie damit nur in die Sicht- und Hörbarkeit für andere Menschen eingewilligt, nicht in die automatisierte Analyse, geschweige denn in die Verwendung für eine polizeiliche Abgleichs-Datenbank. Zudem werden Menschen auch ohne Zustimmung Gegenstand von im Internet veröffentlichten Bildern, beispielsweise als Besucher*innen von Demonstrationen, über die Tageszeitungen berichtet haben.

Das führt direkt zu einem der größten Knackpunkte der Befugnis: Ihren Implikationen für das Versammlungsrecht. Denn mit einer derartigen Gesichtersuchmaschine könnte die Polizei die Teilnehmer*innen einer Demonstration beinahe vollumfänglich identifizieren, sobald dort eine Straftat stattfindet. Dementsprechend ist zu befürchten, dass Menschen von ihrem Recht auf Versammlungsfreiheit allein aufgrund des Wissens um diese Technologie keinen Gebrauch machen.

Ebenso ist es möglich, dass das Recht auf freie Meinungsäußerung eingeschränkt wird, wenn Menschen beispielsweise davor zurückscheuen, einen Podcast aufzunehmen, weil ihre Stimme danach polizeilich genutzt und identifiziert werden könnte.

¹⁴ https://www.bverfg.de/e/rs20181218_1bvr014215.html

Laut einem von AlgorithmWatch beauftragten Gutachten¹⁵ und einer Analyse der Wissenschaftlichen Dienste des Bundestags¹⁶ ist ein biometrischer Abgleich von Informationen gesuchter Personen mit Daten aus dem Internet ohne den Aufbau einer Datenbank nicht sinnvoll möglich. Die Abgleichs-Datenbank, die die Polizei für eine derartige Suche vorhalten oder aufbauen muss, widerspricht dem Verbot der anlasslosen Datenspeicherung, das das Bundesverfassungsgericht in seinem Urteil zur Vorratsdatenspeicherung bestätigt hat,¹⁷ und wohl auch der KI-Verordnung der EU, die das „ungezielte Auslesen“ von biometrischen Daten aus dem Internet mittels KI zum Aufbau einer Datenbank verunmöglicht.

Problematisch an der Befugnis ist auch, dass die Algorithmen diskriminierend wirken. Eine Untersuchung des US-amerikanischen National Institute of Standards and Technology¹⁸ hat ergeben, dass die untersuchten Gesichtserkennungsalgorithmen Menschen je nach Alter, Geschlecht oder Hautfarbe unterschiedlich präzise erkennen. Demnach werden Menschen, die nicht mittelalt, weiß und männlich sind, mit erhöhter Wahrscheinlichkeit Opfer einer Fehlidentifizierung – und der darauf folgenden polizeilichen Maßnahmen.

Ich empfehle, die Befugnis ersatzlos aus dem Entwurf zu streichen.

15 <https://www.algorithmwatch.org/de/gutachten-datenbank-biometrie-gesichtserkennung/>

16 <https://www.bundestag.de/resource/blob/1149732/EU-6-074-25-WD-5-105-25.pdf>

17 https://www.bverfg.de/e/rs20100302_1bvr025608.html

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