Gesellschaft für Freiheitsrechte

freiheitsrechte.org

28. September 2025

Stellungnahme

zum Entwurf der Fraktion der CDU und der Fraktion der SPD

Gesetz zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin

(Abgh-Drs. 19/2553)

David Werdermann

Rechtsanwalt und Verfahrenskoordinator
bei der Gesellschaft für Freiheitsrechte e.V.

A. Zusammenfassung

Ich bedanke mich für die Gelegenheit der Stellungnahme. Die Gesellschaft für Freiheitsrechte setzt sich mit juristischen Mitteln für die Grund- und Menschenrechte ein. In den letzten Jahren hat die Gesellschaft für Freiheitsrechte zahlreiche Verfassungsbeschwerden initiiert und koordiniert, die die Rechtsprechung des Bundesverfassungsgerichts zum Sicherheitsrecht geprägt haben. Dazu zählen die Entscheidungen zum Umgang mit IT-Sicherheitslücken nach dem Polizeigesetz-Baden-Württemberg[1], zum Sicherheits- und Ordnungsgesetz Mecklenburg-Vorpommern[2], zur automatisierten Datenauswertung in Hamburg und Hessen[3], zum Bundeskriminalamtgesetz[4] sowie zu verschiedenen Gesetzen im Nachrichtendienstrecht.[5]

In den meisten Bundesländern wurden in den letzten Jahren die polizeilichen Befugnisse deutlich erweitert.[6] Einerseits wurden bestehende Befugnisse ins Vorfeld einer konkreten Gefahr

[1] BVerfGE 158, 170.
[2] BVerfG, Beschluss des Ersten Senats vom 9. Dezember 2022 - 1 BvR 1345/21.
[3] BVerfG, Urteil des Ersten Senats vom 16. Februar 2023 - 1 BvR 1547/19.
[4] BVerfG, Urteil des Ersten Senats vom 01. Oktober 2024 - 1 BvR 1160/19.
[5] BVerfGE 154, 152 (BND-Ausland-Ausland-Fernmeldeaufklärung); BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 – (Bayerisches Verfassungsschutzgesetz); BVerfG, Beschluss des Ersten Senats vom 17. Juli 2024 - 1 BvR 2133/22 – (Hessisches Verfassungsschutzgesetz); BVerfG, Beschluss des Ersten Senats vom 08. Oktober 2024 - 1 BvR 1743/16 – (BND – Cybergefahren).
[6] Töpfer/Kühne, CILIP 127 (2021), S. 7.

vorverlagert, andererseits wurden neue Befugnisse geschaffen etwa zum Einsatz von Staatstrojanern und Big-Data-Analysen. Zu beobachten ist ein gesetzgeberischer Aktionismus, dessen zentrales Motiv die Inszenierung von Handlungsfähigkeit ist. Die Politik lässt sich von technischen Neuerungen und aufgeheizten Debatten treiben. Das Bundesverfassungsgericht musste mehrmals eingreifen, nicht weil seine Rechtsprechung besonders streng ist, sondern weil die Politik immer wieder an die Grenze des verfassungsrechtlich Zulässigen geht – und oft auch darüber hinaus.

Berlin hat bisher – anders als die meisten anderen Bundesländer – auf eine umfassende Ausweitung polizeilicher Befugnisse verzichtet. Mit dem vorliegenden Gesetzentwurf erfolgt einer Abkehr von dieser grundrechtsfreundlichen Politik. Mit den vorgeschlagenen Änderungen soll weitgehend die Rechtsprechung des Bundesverfassungsgerichts nachgezeichnet werden, was aber nicht durchgehend gelingt. Die maßgeblich aus dem Verhältnismäßigkeitsgrundsatz folgenden Anforderungen an schwere Grundrechtseingriffe werden nicht eingehalten. Zudem werden grundrechtlich hochproblematische neue Instrumente eingeführt. An dieser Stelle möchte ich nur auf einige eingehen:

- Der Gesetzentwurf hält am problematischen Konstrukt der kriminalitätsbelasteten Orte fest. An diesen Orten sollen nicht nur – wie bisher - anlasslose Kontrollen durchgeführt werden, die besonders anfällig für Diskriminierung sind. Stattdessen soll künftig – ebenso wie in und an gefährdeten Objekten sowie bei öffentlichen Veranstaltungen und Ansammlungen - auch **Videoüberwachung** zum Einsatz kommen. Dadurch werden alle Menschen, die sich an solchen Orten aufhalten, unter Generalverdacht gestellt. Eingriffsverstärkend kommt hinzu, dass die Videoaufnahmen mittels Verhaltensmustererkennung automatisiert ausgewertet werden. Es ist zu befürchten, dass gerade Menschen, die sich atypisch im öffentlichen Raum verhalten (z.B. wohnungslose Menschen, Menschen mit körperlichen Einschränkungen) von der eingesetzten Software als „gefährlich" erkannt werden und dadurch erhöhtem Überwachungsdruck ausgesetzt sind. Der Entwurf sieht für die automatisierte Auswertung keine erhöhte Schwelle vor, wie zum Beispiel die Verhütung schwerer Straftaten. Es fehlt zudem an Regeln zur genauen Funktionsweise, zum Ausschluss selbstlernender Künstlicher Intelligenz, zur Verhinderung von Diskriminierung sowie zur verpflichtenden Kontrolle durch die Landesdatenschutzbeauftragte.
- Bei der **Quellen-Telekommunikationsüberwachung und der Online-Durchsuchung** werden Smartphones und PCs mit Hilfe eines Staatstrojaners infiltriert. Angesichts der Vielfalt an Daten, die sich auf informationstechnischen Systemen befinden, greifen beide

Maßnahme besonders schwer in Grundrechte ein. Die Eingriffsschwellen werden dem Eingriffsgericht nicht durchgängig gerecht. Zudem fehlt es an einer unabhängigen Überprüfung der eingesetzten Software. Auf dem Markt gibt es zahlreiche Lösungen, die schlicht nicht den rechtlichen Vorgaben entsprechen, wie zum Beispiel der Pegasus-Trojaner, der auch von autokratischen Regimen genutzt wird. Zudem geht mit den Befugnissen eine Gefahr für IT-Sicherheit einher, weil sie dazu verleiten, Schwachstellen offen zu halten. Diese können dann auch von Kriminellen und ausländischen Geheimdiensten genutzt werden.

- Der nachträgliche **biometrische Abgleich mit öffentlich zugänglichen Daten** hebt faktisch die Anonymität im Internet auf. Jedes Foto, das möglicherweise ohne das Wissen und Einverständnis der betroffenen Person ins Netz gestellt wird, kann zu Überwachungszwecken genutzt werden. Das ist mit enormen Abschreckungseffekten verbunden und hat erhebliche Auswirkungen auf die Ausübung von Grundrechten. Es ist beispielsweise nicht mehr möglich, an einer Versammlung teilzunehmen, ohne damit rechnen zu müssen, dass Fotos, die beispielsweise von der Presse veröffentlicht werden, anschließend von der Polizei für einen Abgleich genutzt werden. Die Vorschrift schließt zudem weder den Aufbau einer biometrischen Referenzdatenbanken auf Vorrat noch die Nutzung von kommerziellen Datenbanken aus. Beides ist jedoch mit der KI-Verordnung und dem Recht auf informationelle Selbstbestimmung nicht vereinbar. Statt konsequent gegen rechtswidrige Angebote wie PimEyes vorzugehen, schafft der Entwurf eine Grundlage für biometrische Massenüberwachung durch die Berliner Polizei.

Diese und andere Verschärfungen lassen eine gewissenhafte Abwägung von Grundrechten vermissen. Der Senat und das Abgeordnetenhaus sollten gerade in Zeiten, in denen die Demokratie und der Rechtsstaat von vielen Seiten angegriffen werden, unbedingt den Eindruck vermeiden, dass sie Grundprinzipien unserer Verfassung systematisch hintanstellen.

B. Rechtliche Bewertung der Regelungen im Einzelnen

Im vorliegenden wird auf einzelne Regelungen näher eingegangen. Dabei wird zwischen breit angelegten offenen Überwachungsmaßnahmen wie Identitätsfeststellungen an kriminalitätsbelasteten Orten sowie Videoüberwachung (**dazu unter I.**) und eingriffsintensiven, verdeckten Maßnahmen (**dazu unter II.**) unterschieden. Abschließend werden einzelne Aspekte von transparenzschaffenden Normen beleuchtet (**dazu unter III.**)

I. Breit angelegte Überwachungsmaßnahmen

1. Maßnahmen an kriminalitätsbelasteten Orten, Diskriminierung (§ 12 Abs. 3, § 17a, § 21 Abs. 2 Satz 1 Nr. 1, § 34 Abs. 2 Nr. 2, § 35 Abs. 2 Nr. 2)

§ 17a[7] regelt die Festlegung **kriminalitätsbelasteter Orte**. An diesen Orten kann die Polizei nach § 21 Abs. 2 Satz 1 Nr. 1 ohne das Vorliegen weiterer Anhaltspunkte die Identität einer Person feststellen und die Person sowie die von ihr mitgeführten Sachen nach § 34 Abs. 2 Nr. 2, § 35 Abs. 2 Nr. 2 durchsuchen. Neu ist die Befugnis zur Datenerhebung (Videoüberwachung) an kriminalitätsbelasteten Orten nach § 24e.[8]

Die Festlegung kriminalitätsbelasteter Orte erfolgt nach der Neuregelung grundsätzlich durch **Rechtsverordnung**. Das stellt eine Verbesserung dar, weil es den Rechtsschutz erleichtert (§ 47 Abs. 1 Nr. 2 VwGO, § 62a JustG Bln) und die genauen Grenzen des Ortes transparent macht.[9]

Das **Regelungskonzept der kriminalitätsbelasteten Orte ist jedoch insgesamt abzulehnen**. Die Effektivität von anlasslosen Identitätsfeststellungen und Durchsuchungen sowie von Videoüberwachung ist fraglich. Die Maßnahmen führen allenfalls dazu, dass Kriminalität sich an andere Orte verlagert.

Orte können nach § 17a Abs. 1 als kriminalitätsbelastet ausgewiesen werden, wenn Tatsachen die Annahme rechtfertigen, dass dort Personen Straftaten von erheblicher Bedeutung verabreden, vorbereiten oder verüben. Die Norm setzt nicht voraus, dass sich die Kriminalitätsbelastung deutlich von anderen (ähnlich stark frequentierten) Orten abhebt. Die konkrete Einstufung erfolgt oft **nicht auf wissenschaftlich fundierter Datengrundlage**, sondern im besten Fall auf Grundlage polizeilicher Statistiken, die durch verschiedene Faktoren, insbesondere die polizeiliche Präsenz, verzerrt sind.[10] Sie kann diskriminierend sein, etwa wenn verstärkt migrantisch geprägte Orte betroffen sind.[11]

Auch die Auswahl der kontrollierten Personen birgt die **Gefahr des Missbrauchs sowie des diskriminierenden Einsatzes der Befugnisse**.[12] Anlasslose Kontrollen könnten zur Einschüchterung bestimmter Gruppen eingesetzt werden. So könnten etwa die Teilnehmer*innen „missliebiger" Versammlungen gezielt und gehäuft angehalten, befragt und durchsucht werden, ebenso Fußballfans auf dem Weg zum Stadion oder bestimmte Gruppen von Wohnungslosen oder

---

[7] §§ ohne Kennzeichnungen sind solche des ASOG nach dem vorliegenden Gesetzentwurf.
[8] Dazu unten I.2.
[9] Nach dem bisherigen § 21 Abs. 4 Satz 1 ASOG wird nur eine „umschreibende Bezeichnung" veröffentlicht.
[10] *Ullrich/Tullney*, sozialraum 2/2012, abrufbar unter https://d-nb.info/1074461746/34.
[11] Heimatkundeboell.de vom 14. April 2021, https://heimatkunde.boell.de/de/2021/04/14/die-kriminalisierung-migrantischer-orte-als-rassistische-praxis.
[12] *Hunold* u.a., Polizei und Diskriminierung, 2025, abrufbar unter https://www.antidiskriminierungsstelle.de/SharedDocs/aktuelles/DE/2025/20250522_Polizeistudie.html.

von Jugendlichen auf öffentlichen Plätzen. Außerdem ist erwiesen, dass anlasslose Kontrollen im besonderen Maße anfällig sind für willentliches oder unwillentliches Racial Profiling.[13] Da auffällige Verhaltensweisen in der Regel bereits eine Gefahr begründen, bleiben für anlasslose Kontrollen fast nur Kriterien, die an das äußere Erscheinungsbild anknüpfen.

Racial Profiling und andere Diskriminierung kann auch die **in § 12 Abs. 3 enthaltene Schutzklausel** nicht verhindern. Ihr kommt zwar als ausdrücklicher Hinweis auf verschiedene Diskriminierungsverbote eine gewisse Warnfunktion zu, jedoch enthält sie keinen über das verfassungsrechtliche Diskriminierungsverbot hinausgehenden Regelungsinhalt und normiert damit keinen besonderen Schutz vor diskriminierenden Maßnahmen. Im Gegenteil droht die Schutzklausel in ihrer bisherigen Formulierung Racial Profiling sogar noch zu befördern: Die vorgeschlagenen Klauseln könnten so verstanden werden, dass eine an ein Merkmal des Art. 3 Abs. 3 GG anknüpfende Personenauswahl bei einem sachlichen Grund eben doch zulässig wäre.[14] So könnten etwa Erkenntnisse zur Häufigkeit der Begehung von Straftaten durch bestimmte ethnische Gruppen als ein sachlicher Grund für eine gezielte Kontrolle dieser Gruppen gewertet werden. Das wäre zwar ungeachtet der fachgesetzlichen Regelung mit Blick auf Art. 3 Abs. 3 GG unzulässig, würde aber eine entsprechende Praxis nicht zuverlässig verhindern.[15] Eine alternative Formulierung wäre etwa: "Bei der Auswahl der von einer Maßnahme betroffenen Person sind die Diskriminierungsverbote aus Artikel 3 Absatz 3 des Grundgesetzes, Artikel 10 Absatz 2 der Verfassung von Berlin und § 2 des Landesantidiskriminierungsgesetzes zu beachten."

Das Risiko diskriminierender Kontrollen könnte durch verpflichtende **Kontrollquittungen** zumindest etwas reduziert werden.[16] Solche Kontrollquittungen sind etwa in § 27 Abs. 1 Satz 2 BremPolG vorgesehen.

---

[13] *Jacobsen/Bergmann*, Diskriminierungsrisiken in der Polizeiarbeit, 2024, S. 131 ff., abrufbar unter https://www.pa.polizei-nds.de/download/77055; *Müller/Wittlif*, Racial Profiling bei Polizeikontrollen. Indizien aus dem SVR-Integrationsbarometer. SVR-Policy Brief 2023-3, Berlin abrufbar unter https://www.svr-migration.de/wp-content/uploads/2023/11/SVR-Policy-Brief_Racial-Profiling-bei-Polizeikontrollen.pdf; *Hunold/Wegener*, APuZ 42–44/2020, S. 27.

[14] Kritisch zum ähnlichen § 5 Abs. 1 LADG auch *Beckmann*, in: Klose/Liebscher/Wersig/Wrase, LADG Berlin, 2025, § 5 Rn. 7 f.

[15] Ähnlich die Stellungnahme der Unabhängigen Bundesbeauftragten für Antidiskriminierung zum Entwurf eines Gesetzes zur Neustrukturierung des Bundespolizeigesetzes (BPolG) und Änderung anderer Gesetze, 20. Dezember 2023, S. 3, abrufbar unter https://www.antidiskriminierungsstelle.de/SharedDocs/downloads/DE/Sonstiges/20231218_stellungnahme_ubad_bpolg.html.

[16] Stellungnahme der Unabhängigen Bundesbeauftragten für Antidiskriminierung zum Entwurf eines Gesetzes zur Neustrukturierung des Bundespolizeigesetzes (BPolG) und Änderung anderer Gesetze, 20. Dezember 2023, S. 2, abrufbar unter https://www.antidiskriminierungsstelle.de/SharedDocs/downloads/DE/Sonstiges/20231218_stellungnahme_ubad_bpolg.html.

2. Videoüberwachung und automatisierte Auswertung

Die §§ 24, 24a und 24e ermöglichen jeweils breit angelegte **Videoüberwachung**. § 24 ermöglicht die Videoüberwachung bei öffentlichen Veranstaltungen und Ansammlungen, die nicht dem Versammlungsfreiheitsgesetz unterliegen. § 24a regelt die Videoüberwachung an gefährdeten Objekten und erweitert die Befugnis auf den Innenraum sowie auf die zugehörigen Parkplätze und sonstige Außenflächen. Das ist bedenklich, weil die dort erhobenen Daten mitunter sensibel sind. So können zum Beispiel religiöse Stätten oder Redaktionsräume gefährdete Objekte sein. § 24e ist neu und ermöglicht die Videoüberwachung an kriminalitätsbelasteten Orten.

Die Videoüberwachung greift intensiv in das **Grundrecht auf informationelle Selbstbestimmung** ein. Sie beeinträchtigt alle, die die betroffenen Orte besuchen, und dient dazu, belastende hoheitliche Maßnahmen vorzubereiten und das Verhalten der den Raum nutzenden Personen zu lenken. Die Videoüberwachung und die Aufzeichnung des gewonnenen Bildmaterials erfassen daher – wie bei solchen Maßnahmen stets – überwiegend Personen, die selbst keinen Anlass schaffen, dessentwegen die Überwachung vorgenommen wird.[17]

Die **Voraussetzungen der Ermächtigungsgrundlagen** werden diesem Eingriffsgewicht nicht gerecht. Hinsichtlich der kriminalitätsbelasteten Orte wird auf die bereits ausgeführte Kritik verwiesen.[18] Die anderen Ermächtigungen sind noch weiter. Die Videoüberwachung bei Veranstaltungen und Ansammlungen ist nach § 24 Abs. 1 Satz 1 bereits zulässig, wenn Tatsachen die Annahme rechtfertigen, dass dabei Straftaten begangen werden. Eine Einschränkung auf erhebliche Straftaten wie bei den kriminalitätsbelasteten Orten fehlt. Nach dem Wortlaut genügt damit der Verdacht, dass Bagatellstraftaten begangen werden. Für § 24a Abs. 1 Satz 1 gilt dasselbe, wobei hier eine abweichende Formulierung gewählt wurde. Tatsächliche Anhaltspunkte müssen die Annahme rechtfertigen, dass an oder in einem Objekt dieser Art Straftaten „drohen". Damit wird die Eingriffsschwelle weiter verwässert.

Das Eingriffsgewicht wird deutlich dadurch erhöht, dass die Aufnahmen nach § 24 Abs. 1 Satz 3, § 24a Abs. 1 Satz 2 und § 24e Abs. 4 **automatisiert ausgewertet** werden können. Das Bundesverfassungsgericht hat bereits zur manuellen Auswertung entschieden, dass diese das Eingriffsgewicht der Videoüberwachung erhöht.[19] Die automatisierte Analyse der Daten hat als Eingriff ein Eigengewicht, das über die über das Gewicht der einfachen Videoüberwachung hinausgeht.[20] Dies liegt daran, dass die weitere Verarbeitung durch eine automatisierte Datenanalyse oder -auswertung **spezifische Belastungseffekte** haben kann.[21] Automatisierte

---

[17] BVerfG, Beschluss der 1. Kammer des Ersten Senats vom 23. Februar 2007 - 1 BvR 2368/06 -, Rn. 52.
[18] Siehe oben I.1.
[19] BVerfG, Beschluss der 1. Kammer des Ersten Senats vom 23. Februar 2007 - 1 BvR 2368/06 -, Rn. 52.
[20] *Bäuerle*, in: BeckOK PolR Hessen, 34. Auflage 15.2.2025, HSOG § 14 Rn. 53.
[21] BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19.

Auswertung bergen stets Diskriminierungsrisiken und sind fehleranfällig. Es steht zu befürchten, dass gerade Menschen, die sich atypisch im öffentlichen Raum verhalten (wohnungslose Menschen, Menschen mit körperlichen Einschränkungen) von der eingesetzten Software als „gefährlich" erkannt werden und dadurch erhöhtem Überwachungsdruck ausgesetzt sind. Sofern private Anbieter eingebunden werden, besteht zudem ein erhöhtes Missbrauchspotenzial.[22] Insgesamt führt die Verhaltenserkennung zu starken **chilling effects** für alle Personen im öffentlichen Raum.

Die Ermächtigungen werden diesem erhöhten Eingriffsgewicht nicht gerecht. Die **Eingriffsschwelle** ist dieselbe wie bei der „normalen" Videoüberwachung. Insbesondere erfolgt keine Eingrenzung auf Orte, an denen schwere Straftaten drohen. Es ist auch unklar, welche Straftaten und welche Unglücksfälle überhaupt durch eine Verhaltensmustererkennung erkannt werden können. Es ist jedoch Aufgabe des Gesetzgebers hierzu Vorgaben zu machen. Die Details und die konkreten Verhaltensmuster müssten gegebenenfalls in einer Rechtsverordnung festgelegt werden.[23]

Die Norm schließt nicht den Einsatz (selbstlernender) **künstlicher Intelligenz** aus.[24] Damit droht die Verdachtsgenerierung gänzlich undurchschaubar und unkontrollierbar zu werden. Es fehlt zudem an einer Regelung zur Vermeidung von Diskriminierung und an verpflichtenden Kontrollen durch die Landesbeauftragte für den Datenschutz.[25] Die Regelungen sind daher insgesamt unverhältnismäßig und verstoßen gegen das Grundrecht auf informationelle Selbstbestimmung.

3. Dash- und Bodycams (§ 24c)

In § 24c wurden die Voraussetzungen für die Nutzung von Dash- und Bodycams geändert. Erforderlich ist danach, dass 1. tatsächliche Anhaltspunkte für die Entstehung einer Gefahr für Leib, Leben oder Freiheit der Person bestehen und 2. die Maßnahme zur Abwehr dieser Gefahr erforderlich erscheint. Laut der Entwurfsbegründung soll damit die konkretisierte Gefahr im Sinne der Rechtsprechung des Bundesverfassungsgerichts umschrieben werden. Jedoch wird nicht die sonst übliche Formulierung gewählt,[26] sondern an eine unscharfe „Entstehung einer Gefahr" angeknüpft. Damit weicht der Entwurf von der Empfehlung der Evaluation nach § 24c Abs. 10 ASOG ab. Im Abschlussbericht wird geraten, die Befugnis tatbestandlich auf den Begriff der konkreten

---

[22] Hamburg setzt etwa Kameras des chinesischen Herstellers Hikvision ein, der für Menschenrechtsverletzungen bekannt ist, vgl. netzpolitik vom 2. September 2025, https://netzpolitik.org/2025/hikvision-hersteller-der-hamburger-ki-ueberwachungskameras-ist-fuer-menschenrechtsverletzungen-bekannt/.

[23] Vgl. dazu BVerfG, Urteil des Ersten Senats vom 16. Februar 2023 - 1 BvR 1547/19 -, Rn. 112 ff.

[24] Vgl. dazu BVerfG, Urteil des Ersten Senats vom 16. Februar 2023 - 1 BvR 1547/19 -, Rn. 121.

[25] Vgl. dazu BVerfG, Urteil des Ersten Senats vom 16. Februar 2023 - 1 BvR 1547/19 -, Rn. 109.

[26] Siehe dazu unten II.1.b.aa.

Gefahr umzustellen.[27] Bedenklich erscheint auch die Formulierung in § 24c Abs. 1 Nr. 2. Der Begriff „erscheint" ist hochgradig unbestimmt.

Der in § 24c Abs. 8 geregelte Gerichtsvorbehalt für die Nutzung von Daten, die an nicht öffentlich zugänglichen Orten entstanden sind, wird durch den Entwurf verschlimmbessert. Bisher war unklar, ob nur die Rechtmäßigkeit der weiteren Nutzung prüfen musste oder auch die Rechtmäßigkeit der Erhebung. Die Evaluation empfahl daher eine gesetzliche Klarstellung, dass *auch* die Rechtmäßigkeit der Erhebung vom Gericht zu prüfen ist.[28] Nach dem Gesetzentwurf ist *nur noch* die Rechtmäßigkeit der Erhebung, nicht mehr die Rechtmäßigkeit der Nutzung zu prüfen. Das wurde weder von der Evaluation empfohlen noch ist es mit dem Wohnungsgrundrecht vereinbar.

II. Verdeckte, eingriffsintensive Überwachungsmaßnahmen

Die §§ 25 ff. enthalten verschiedene Befugnisse für verdeckte eingriffsintensive Überwachungsmaßnahmen. Den Befugnissen sind verschiedene Mängel hinsichtlich der zu schützenden Rechtsgüter, der Eingriffsschwellen und der Subsidiarität gemein, die vorab erläutert werden (**dazu unter 1.**). Anschließend wird auf einzelne Befugnisse eingegangen (**dazu unter 2. Bis 9.**).

1. Übergreifende Probleme

Besonders eingriffsintensive Maßnahmen sind nach der Rechtsprechung des Bundesverfassungsgerichts grundsätzlich nur bei Vorliegen einer mindestens konkretisierten Gefahr für ein besonders gewichtiges Rechtsgut zulässig. Das Bundesverfassungsgericht stellt somit Anforderungen sowohl an die zu schützenden Rechtsgüter (**dazu unter a.**) als auch an die Eingriffsschwelle (**dazu unter b.**) die nur teilweise eingehalten werden. Zu kritisieren ist zudem die neue einheitliche Subsidiaritätsklausel (**dazu unter c.**).

a. Rechtsgüter

Zu den **besonders gewichtigen Rechtsgütern** gehören Leib, Leben und Freiheit der Person sowie der Bestand oder die Sicherheit des Bundes oder eines Landes. Darüber hinaus kann auch der Schutz von Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, besonders schwere Grundrechtseingriff rechtfertigen. Dabei ist jedoch ein enges Verständnis

[27] Law & Society Institute, Bodycams bei der Polizei Berlin und der Berliner Feuerwehr, 2024, S. 28, abrufbar unter https://www.parlament-berlin.de/ados/19/InnSichO/vorgang/iso19-0207-Abschlussbericht%20Evaluation%20Bodycams.pdf.
[28] Law & Society Institute, Bodycams bei der Polizei Berlin und der Berliner Feuerwehr, 2024, S. 41, S. 127, abrufbar unter https://www.parlament-berlin.de/ados/19/InnSichO/vorgang/iso19-0207-Abschlussbericht%20Evaluation%20Bodycams.pdf.

geboten. Gemeint sind etwa wesentliche Infrastruktureinrichtungen oder sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen.[29]

Der Gesetzentwurf orientiert sich in vielen Vorschriften an diesen Rechtsgütern und ergänzt sie teilweise um die sexuelle Selbstbestimmung.[30] Beim Rechtsgut der sexuellen Selbstbestimmung wird teilweise auch die **Intensität der drohenden Verletzung** mit in den Blick genommen.[31] Das ist grundsätzlich eine Regelungstechnik, die eine stärkere Steuerungswirkung entfaltet und damit dem Verhältnismäßigkeitsgrundsatz Rechnung trägt. Eine entsprechende Einschränkung ist auch bei den Rechtsgütern der körperlichen Integrität (Leib) und der Freiheit der Person (Freiheit) angezeigt. Im Gesetzentwurf sollte zudem „Freiheit" durch „Freiheit der Person" ersetzt werden, um deutlich zu machen, dass nicht jede Einschränkung der allgemeinen Handlungsfreiheit ausreicht.[32] Als Vorlage kann insofern § 19 Abs. 3 Nr. 4 BVerfSchG dienen. Danach gehört zu den besonders gewichtigen Rechtsgütern „das Leben sowie bei einer erheblichen Gefährdung im Einzelfall die körperliche Integrität und die Freiheit einer Person".

Laut Bundesverfassungsgericht kann der Gesetzgeber darauf verzichten, das erforderliche Rechtsgut unmittelbar zu benennen und stattdessen an Straftaten anknüpfen, deren Verhütung mit der Befugnis bezweckt wird. Dem verfassungsrechtlichen Erfordernis eines besonders gewichtigen Rechtsguts entspricht jedenfalls eine Begrenzung auf **besonders schwere Straftaten** im verfassungsrechtlichen Sinn, also zunächst solche, die mit einer Höchstfreiheitsstrafe von mehr als fünf Jahren bedroht sind. Grundsätzlich kann aber auch eine Straftat mit einer angedrohten Höchstfreiheitsstrafe von mindestens fünf Jahren als besonders schwer eingestuft werden, wenn dies nicht nur unter Berücksichtigung des jeweils geschützten Rechtsguts und dessen Bedeutung für die Rechtsgemeinschaft, sondern auch unter Berücksichtigung der Tatbegehung und Tatfolgen vertretbar erscheint.[33] Zudem ist zu fordern, dass die in Bezug genommenen Straftaten dem Schutz eines besonders gewichtigen Rechtgutes dienen.[34]

Der Gesetzentwurf knüpft an verschiedenen Stellen an die **Straftatenkataloge in § 100a Abs. 2 und § 100b Abs. 2 StPO** an.[35] Das ist in zweierlei Hinsicht nicht mit den verfassungsrechtlichen Vorgaben vereinbar.

---

[29] BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025 - 1 BvR 2466/19 -, Rn. 135 m.w.N.
[30] Beispielhaft § 25 Abs. 1 Nr. 1 Buchst. a.
[31] Beispielhaft § 26e Abs. 1 Satz 1 Nr. 1.
[32] Vgl. zu „Straftaten gegen die Freiheit": BVerfG, Beschluss des Ersten Senats vom 17. Juli 2024 - 1 BvR 2133/22 -, Rn. 217.
[33] BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025 - 1 BvR 2466/19 -, Rn. 137.
[34] BVerwG, Beschluss vom 31.05.2022 - 6 C 2.20, Rn. 31 ff.
[35] Beispielhaft § 25a Abs. 2.

Erstens handelt es sich **nicht durchgängig um besonders schwere Straftaten**. Das hat das Bundesverfassungsgericht jüngst zu § 100a Abs. 2 StGB festgestellt.[36] Aber auch bei dem engeren Katalog des § 100b Abs. 2 StPO sind die oben genannten Kriterien nicht durchgängig erfüllt. Insbesondere werden auch Delikte erfasst, die Vermögen und Eigentum schützen oder die im Höchstmaß mit einer Freiheitsstrafe von nur fünf Jahren bedroht sind, ohne dass eine Einstufung als besonders schwer vertretbar wäre.[37]

Zweitens dürfte es sich um **dynamische Verweisungen** handeln. Weder dem Wortlaut noch der Entwurfsbegründung ist zu entnehmen, dass auf § 100a Abs. 2 und § 100b Abs. 2 StPO nur in der aktuellen bundesgesetzlichen Fassung verwiesen werden soll. Dynamische Verweisungen des Landesgesetzgebers auf bundesgesetzliche Normen sind jedoch nur ausnahmsweise dann möglich, wenn die in Bezug genommenen Regelungen ein eng umrissenes Feld betreffen und deren Inhalt im Wesentlichen bereits feststeht.[38] Das ist bei den Verweisen auf § 100a Abs. 2 und § 100b Abs. 2 StPO nicht der Fall. Da das Sicherheitsrecht ein Feld intensiver politischer Auseinandersetzung ist, sind Änderungen der Straftatenkataloge schwer abzusehen.[39]

b. Eingriffsschwellen

aa. Konkretisierte Gefahr

Das Bundesverfassungsgericht verlangt bei eingriffsintensiven Maßnahmen wenigstens eine **konkretisierte Gefahr**. Hierzu müssen grundsätzlich zwei Bedingungen erfüllt sein: Die Tatsachen müssen dafür zum einen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, zum anderen darauf, dass bestimmte Personen beteiligt sein werden, über deren Identität zumindest so viel bekannt ist, dass die Überwachungsmaßnahme gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden kann.[40]

Der Entwurf orientiert sich an verschiedenen Stellen erkennbar an dieser Rechtsprechung, ignoriert jedoch die zweite Bedingung.[41]

---

[36] BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025 - 1 BvR 180/23 -, Rn. 215 ff.
[37] Ausführlich dargelegt in der Verfassungsbeschwerde gegen Art. 61a Abs. 2 Satz 1 Br. 1 BayPAG, S. 129 ff., abrufbar unter https://freiheitsrechte.org/uploads/documents/Freiheit-im-digitalen-Zeitalter/Verfassungsbeschwerde-Art.-61a-BayPAG/2025-07-23-Verfassungsbeschwerde-Art.-61a-BayPAG_geschwaerzt.pdf.
[38] BVerfGE 162, 1 (169 f. Rn. 385) m.w.N.
[39] BVerfGE 162, 1 (170 Rn. 386 m.w.N.) zu einem dynamischen Verweis auf § 100b Abs. 2 StPO in einer sicherheitsrechtlichen Ermächtigungsgrundlage; siehe auch die Verfassungsbeschwerde gegen Art. 61a Abs. 2 Satz 1 Br. 1 BayPAG, S. 125 ff., abrufbar unter https://freiheitsrechte.org/uploads/documents/Freiheit-im-digitalen-Zeitalter/Verfassungsbeschwerde-Art.-61a-BayPAG/2025-07-23-Verfassungsbeschwerde-Art.-61a-BayPAG_geschwaerzt.pdf.
[40] BVerfGE 141, 220 (272 f. Rn. 112); BVerfG, Beschluss des Ersten Senats vom 14. November 2024 - 1 BvL 3/22 -, Rn. 77.
[41] Beispielhaft § 25 Abs. 1 Satz 1 Nr. 1 Buchst. b, § 47a Abs. 1 Satz 2 Nr. 2.

bb. Personenbezogen konkretisierte Gefahr

Eine weitere Absenkung der Anforderungen an die Vorhersehbarkeit des Geschehensablaufs kann dem Bundesverfassungsgericht zufolge verfassungsmäßig sein, wenn das **individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie in überschaubarer Zukunft Straftaten begehen wird**.[42]

Hierbei handelt es sich jedoch um eine Ausnahme, die **auf drohende terroristische Straftaten beschränkt** ist.[43] Das ergibt sich bereits aus dem Wortlaut der entsprechenden Entscheidungen des Bundesverfassungsgerichts. Die Fallgruppe hat das Gericht „in Bezug auf terroristische Straftaten" entwickelt.[44] Die Anforderungen an die konkretisierte Gefahr könnten „zur Verhütung terroristischer Straftaten" abgesenkt werden.[45] Die Beschränkung auf terroristische Straftaten ergibt sich auch aus der Begründung, die das Bundesverfassungsgericht für die Absenkung der Anforderungen an die Vorhersehbarkeit des Geschehensablauf nennt. Terroristische Straftaten würden oft als lange geplante Taten von bisher nicht straffällig gewordenen Einzelnen an nicht vorhersehbaren Orten und in ganz verschiedener Weise verübt.[46] Entscheidend ist demnach nicht allein, dass schwere Straftaten beziehungsweise Schäden für herausgehobene Rechtsgüter drohen. Vielmehr rechtfertigt sich die Absenkung der Anforderungen an die Vorhersehbarkeit gerade des Geschehensablaufs dadurch, dass bei terroristischen Straftaten schwerwiegende Rechtsgutsbeeinträchtigungen drohen, deren konkreter Ablauf regelmäßig erst unmittelbar vor ihrer Ausführung absehbar ist. Zugleich ist bei Verhaltensweisen, die auf drohende terroristische Straftaten hindeuten, regelmäßig absehbar, *dass* schwerwiegende Rechtsgutsbeeinträchtigungen zu erwarten sind. Unsicher ist das *wie*, nicht das *ob* der Angriffe. Allein diese Besonderheit einer hohen Wahrscheinlichkeit schwerwiegender Angriffe, deren konkreter Ablauf jedoch typischerweise erst unmittelbar vor ihrer Ausführung erkennbar ist, rechtfertigt es, das mit der Unklarheit über das zu erwartende Geschehen verbundene Risiko von Fehleinschätzungen in Kauf zu nehmen.[47]

Der Entwurf knüpft in vielen Normen an die drohende Begehung terroristischer Straftaten an,[48] in manchen Regelungen weicht er hiervon jedoch ab.[49] Die Behauptung in der Entwurfsbegründung, dass bestimmte schwere, nicht-terroristische Straftaten oftmals von Einzelnen in einer kaum

---

[42] BVerfGE 165, 1 (50); 155, 119 (188); 141, 220 (272 f., 291).
[43] BayVerfGH, Entscheidung vom 13. März 2025 – Vf. 5-VIII-18 –, Rn. 187.
[44] BVerfGE 141, 220 (272).
[45] So BVerfG, Beschluss vom 14. November 2024 – 1 BvL 3/22 –, Rn. 78.
[46] So BVerfGE 169, 332 (376); 165, 1 (50); 141, 220 (272).
[47] Vgl. zu diesem Risiko BVerfGE 113, 348 (386); Sächsischer Verfassungsgerichtshof, Urteil vom 25. Januar 2024 –Vf. 91-II-19 –, Rn. 161.
[48] § 26e Abs. 1 Satz 1 Nr. 3, § 28a Abs. 1 Satz 1 Nr. 3, § 47a Abs. 1 Satz 2 Nr. 3.
[49] § 26c Abs. 2 Satz 1 Nr. 3 und Nr. 5, Abs. 4 Satz 1 Nr. 3, § 26d Abs. 5 Satz 1 Nr. 3 und Nr. 5, § 29b Abs. 1 Satz 1 Nr. 2.

konkret vorhersehbaren Weise verübt würden,[50] wird nicht näher begründet und rechtfertigt kein pauschales Absenken der Anforderungen an die Vorhersehbarkeit des Geschehensverlaufs.

cc. Bezugnahme auf Vorfelddelikte

Ein besonderes Problem ergibt sich bei der Bezugnahme auf Straftatbestände, bei denen die Strafbarkeitsschwelle durch die Einbeziehung von **Vorbereitungshandlungen in das Vorfeld von konkreten Rechtsgutsgefahren oder -verletzungen** verlagert wird. Hier muss der Gesetzgeber nach der Rechtsprechung des Bundesverfassungsgerichts sicherstellen, dass in jedem Einzelfall eine konkrete oder konkretisierte Gefahr für die durch den Straftatbestand geschützten Rechtsgüter vorliegt.[51] Der Entwurf versucht, diese Vorgaben in § 17 Abs. 6 umzusetzen. Das gelingt jedoch nicht.

Erstens werden nicht alle Vorfelddelikte erfasst. Nicht genannt wird beispielsweise die von § 100a Abs. 2 Nr. 1 Buchst. d StPO erfasste **Bildung einer kriminellen Vereinigung nach § 129 StGB**, obwohl auch dieser Tatbestand die Strafbarkeitsschwelle ins Vorfeld einer Rechtsgutsverletzung verlagert. Ausreichend ist nach § 129, dass Zweck oder Tätigkeit der Vereinigung auf die Begehung von Straftaten *gerichtet ist*.

Zweitens ist das „durch den jeweiligen Straftatbestand geschützte **Rechtsgut**" nicht immer einfach zu bestimmen. So soll das Schutzgut von § 129a StGB die „öffentliche Sicherheit", der „öffentliche Friede", oder die „innere Sicherheit" sein.[52] Hierbei ist bereits fraglich, ob es sich überhaupt um Rechtsgüter handelt, jedenfalls handelt es sich nicht um besonders gewichtige Rechtsgüter. Folgt man der Gegenauffassung und stellt auf die Bezugsstraftaten des § 129a StGB ab, sind die Rechtsgüter einfacher zu bestimmen. Jedoch stellt sich dann die Frage, wozu es einer Bezugnahme auf das Vorfelddelikt überhaupt bedarf.

Schließlich stellt die „vor die Klammer gezogene" Begriffsbestimmung in § 17 Abs. 6 nicht hinreichend sicher, dass Normanwender*innen sich der Einschränkung in jedem Fall bewusst sind. Stattdessen **sollte ganz darauf verzichtet werden, auf Vorfelddelikte Bezug zu nehmen**. Bei verfassungskonformer Auslegung dürfte die Bezugnahme ohnehin weitgehend leerlaufen.

c. Subsidiarität

In den §§ 25 bis 26 soll eine einheitliche Subsidiaritätsklausel verwendet werden. Das ist zu begrüßen, jedoch entscheidet sich der Entwurf für eine Formulierung, die eine „zugespitzte Form der Erforderlichkeit"[53] aufzuweichen droht. Danach setzt der Einsatz besonders eingriffsintensiver

---

[50] Gesetzentwurf, S. 249.
[51] BVerfG, Urteil des Ersten Senats vom 16. Februar 2023 - 1 BvR 1547/19 -, Rn. 170.
[52] Vgl. *Eschelbach*, in: NK-StGB, 6. Aufl. 2023, § 129a Rn. 14.
[53] *Graulich*, in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, 2. Aufl. 2018, BPolG § 21 Rn. 1; *Schulenberg*, in: NK-BKAG, 1. Aufl. 2023, BKAG § 45 Rn. 75.

Mittel nicht mehr – wie bisher in § 25a Abs. 1 Satz 1 ASOG – voraus, dass die „Abwehr der Gefahr oder Verhütung der Straftaten auf andere Weise aussichtslos oder wesentlich erschwert wäre". Genügen soll stattdessen, dass die Abwehr der Gefahr oder Verhütung der Straftaten auf andere Weise aussichtslos „erscheint".[54] Welche Bedeutung diese abgeschwächte Formulierung hat, wird nicht erläutert.[55] Es ist zu befürchten, dass sich Polizeibeamte künftig auf vage Erfahrungswerte berufen, um mildere Mittel von vorneherein als „aussichtslos erscheinend" darzustellen.

2. Datenerhebung durch längerfristige Observation (§ 25)

Observationen können sehr intensiv in Grundrechte eingreifen. Das gilt insbesondere, wenn sie über einen längeren Zeitraum oder in Kombination mit Bild- oder Tonaufzeichnungen erfolgen.[56] Aus diesem Grund sind im Entwurf für das Berliner Verfassungsschutzgesetz strenge Voraussetzungen vorgesehen, wenn die Observation durchgehend länger als eine Woche dauert oder an mehr als 14 Tagen innerhalb eines Monats oder unter Einsatz technischer Mittel außerhalb der Öffentlichkeit stattfindet.[57] Dem Eingriffsgewicht entspricht es im Polizeirecht die Befugnis auf den Schutz besonders gewichtiger Rechtsgüter beziehungsweise auf die Verhütung besonders schwerer Straftaten zu begrenzen.[58]

§ 25 Abs. 1 Satz 1 Nr. 1 Buchst. b wird dem nicht gerecht. Die Norm nimmt Bezug auf Straftaten mit erheblicher Bedeutung gemäß § 17 Abs. 3. Es wird also noch nicht einmal auf den Katalog des § 100a Abs. 2 StPO geschweige denn auf den Katalog des § 100b Abs. 2 StPO oder die Definition terroristischer Straftaten in § 17 Abs. 5 verwiesen.

§ 25 Abs. 1 Satz 1 Nr. 2 ermöglicht die Observation von **Kontakt- und Begleitpersonen**. Will der Gesetzgeber auf eine solche Überwachung von unbeteiligten Dritten nicht verzichten, sollte zumindest mit einem Klammerzusatz auf die Legaldefinition in § 18 Abs. 2 Nr. 1 Buchst. b verwiesen werden, um die Normanwendung zu erleichtern.

Außerdem entspricht die Definition in § 18 Abs. 2 Nr. 1 Buchst. b nicht den verfassungsrechtlichen Anforderungen. Zwar ist auch der Einsatz einer eingriffsintensiven Überwachungsmaßnahme unmittelbar gegenüber Kontaktpersonen nicht schlechthin ausgeschlossen. Er steht aber unter strengen Verhältnismäßigkeitsanforderungen und setzt eine spezifische individuelle Nähe der Betroffenen zu der die Überwachung der verantwortlichen Person rechtfertigenden

[54] Siehe beispielhaft § 25 Abs. 1 Satz 2.
[55] Gesetzentwurf S. 177.
[56] Vgl. BVerfG, Beschluss des Ersten Senats vom 14. November 2024 - 1 BvL 3/22 -, Rn. 93 ff.; BVerfG, Beschluss des Ersten Senats vom 17. Juli 2024 - 1 BvR 2133/22 -, Rn. 96; BVerfG, Urteil des Ersten Senats vom 26. April 2022 - 1 BvR 1619/17 -, Rn. 357.
[57] AbgH-Drs. 19/2466, § 28 Abs. 2 Satz 2 VSG Bln-E.
[58] BVerwG, Beschluss vom 31.05.2022 - 6 C 2.20, Rn. 31; vgl. auch BVerfG, Beschluss des Ersten Senats vom 14. November 2024 - 1 BvL 3/22 -, Rn. 97.

aufzuklärenden Gefahr voraus.[59] Für die Überwachung Dritter bedarf es daher Anhaltspunkte, dass der Kontakt einen Bezug zum Ermittlungsziel aufweist und so eine nicht unerhebliche Wahrscheinlichkeit besteht, dass die Überwachungsmaßnahme der Aufklärung der Gefahr dienlich sein wird.[60] Bei § 45 Abs. 1 Satz 1 Nr. 4 BKAG ist diese Anforderung gewahrt, wenn man die Norm verfassungskonform auslegt und die dort genannten Nähekriterien als „eigene, in den Gründen der Anordnung darzulegende Voraussetzung für entsprechende Maßnahmen" versteht.[61]

§ 18 Abs. 2 Nr. 1 Buchst. b nennt auch eines der Nähekriterien („Tatsachen die Annahme rechtfertigen, dass eine in Buchstabe a genannte Person sich dieser Person zur Begehung dieser Straftaten bedienen könnte"), allerdings als Regelbeispiel („insbesondere weil"). Die allgemeine Voraussetzung („mit einer in Buchstabe a genannten Person nicht nur in einem flüchtigen oder zufälligen Kontakt, sondern in einer Weise in Verbindung steht, die die Erhebung ihrer personenbezogenen Daten zur vorbeugenden Bekämpfung solcher Straftaten erfordert") benennt keine hinreichend bestimmte Nähekriterien.

Erst recht wird § 25 Abs. 1 Satz 1 Nr. 3 den verfassungsrechtlichen Anforderungen gerecht. Hier wird die die Überwachung ins Blaue hinein auf jede „**andere Person**" erstreckt. Das Vorliegen einer gegenwärtigen Gefahr für besonders gewichtige Rechtsgüter befreit nicht von der Pflicht, die Überwachung auf Personen zu begrenzen, die eine Nähe zu der Gefahr aufweisen.

3. Datenerhebung durch den verdeckten Einsatz technischer Mittel außerhalb von Wohnungen (§ 25a)

§ 25a regelt den verdeckten Einsatz technischer Mittel außerhalb von Wohnungen. Auch diese Maßnahmen können bei entsprechender Dauer schwerwiegend in Grundrechte eingreifen.[62] Die Befugnis ist jedoch durch den Verweis auf die Voraussetzungen des § 25 Abs. 1 **nicht auf den Schutz besonders gewichtiger Rechtsgüter bzw. die Verhütung besonders schwerer Straftaten beschränkt**.[63] Zudem ist die Regelung nicht hinreichend bestimmt, soweit sie die technischen Mittel beziehungsweise deren Einsatzmöglichkeiten nicht abschließend regelt („insbesondere zur").

Für den verdeckten Einsatz technischer Mittel zur Anfertigung von Bildaufnahmen oder -aufzeichnungen, der nicht durchgehend länger als 24 Stunden oder an mehr als zwei Tagen erfolgt, werden die Anforderungen in § 25a Abs. 1 Satz 2 sogar noch weiter heruntergesetzt. Hier wird nicht mehr auf Straftaten von erheblicher Bedeutung, sondern auf alle Straftaten Bezug genommen.

---

[59] BVerfG, Urteil des Ersten Senats vom 01. Oktober 2024 - 1 BvR 1160/19 -, Rn. 109.
[60] BVerfGE 141, 220 (Rn. 116).
[61] BVerfGE 141 220 (Rn. 168).
[62] BVerfG, Beschluss des Ersten Senats vom 14. November 2024 - 1 BvL 3/22 -, Rn. 93 ff.
[63] Siehe oben II.2.

Hierzu zählen Bagatellstraftaten wie das Erschleichen von Leistungen (§ 265a StGB). Soweit in der Norm ausgeschlossen wird, dass die Maßnahme der „Erstellung eines Bewegungsbilds dient", ist darauf hinzuweisen, dass sich das Eingriffsgewicht nach der bundesverfassungsgerichtlichen Rechtsprechung nicht danach bestimmt, von welchen Nutzungsmöglichkeiten die Behörde tatsächlich Gebrauch machen will, sondern danach, welche Nutzungsmöglichkeiten die Regelung rechtlich und tatsächlich eröffnet, also den aktuellen Eingriffsmöglichkeiten.[64] Es kommt nicht darauf an, ob die Maßnahme der Erstellung eines Bewegungsbilds *dient*, sondern ob sie dies *ermöglicht*. Aus diesem Grund ist auch der Gerichtsvorbehalt in § 25a Abs. 3 Satz 1 Nr. 1 unzureichend.

§ 25a Abs. 2 beschränkt das Abhören oder Aufzeichnen des nicht öffentlich gesprochenen Wortes immerhin auf die Verhütung von Straftaten nach § 100a Abs. 2 StPO. Aber auch das ist angesichts des erheblichen Eingriffsgewichts unzureichend.[65]

4. Verdeckter Einsatz technischer Mittel zur Erhebung von Daten in oder aus Wohnungen (§ 25b)

Mit § 25b regelt die Wohnraumüberwachung. Die Vorschrift ist rechtlichen Bedenken ausgesetzt.

Die **Adressat*innenregelung** in § 25b Abs. 1 Satz 1 Nr. 2 Buchst. b ist systemwidrig. Zwar wurde eine vergleichbare Norm vom Bundesverfassungsgericht gebilligt.[66] Jedoch setzt § 25b Abs. 1 Satz 1 Nr. 1 eine gegenwärtige beziehungsweise dringende Gefahr voraus und verlagert die Eingriffsschwelle im Einklang mit Art. 13 Abs. 4 ins Vorfeld der konkreten Gefahr. Der Zweck der Adressat*innenregelung erschließt sich daher nicht.

Sehr problematisch ist auch die Vorschrift des § 25b Abs. 1 Satz 3. Danach gilt § 36 Abs. 5 entsprechend, soweit die Datenerhebung nicht mit technischen Mitteln erfolgt. § 36 Abs. 5 regelt ein Betretungsrecht für Betriebs- und Geschäftsräume, das laut Bundesverfassungsgericht einem eigenständigen Schrankenregime unterfällt.[67] Ob § 36 Abs. 5 den verfassungsrechtlichen Anforderungen genügt, ist fraglich. Insbesondere ist zweifelhaft, ob die Norm den Zweck des Betretens, den Gegenstand und den Umfang der zugelassenen Besichtigung und Prüfung deutlich erkennen lässt.[68] Jedenfalls können verdeckte Maßnahmen nicht vom Betretungsrecht erfasst sein. Es besteht eine Informationspflicht.[69] § 25b Abs. 1 Satz 3 soll demgegenüber **heimliche**

[64] BVerfG, Beschluss des Ersten Senats vom 17. Juli 2024 - 1 BvR 2133/22 -, Rn. 145.
[65] Siehe oben II.1.a. und b.cc..
[66] BVerfGE 141, 220 (Rn. 189 f.).
[67] BVerfGE 32, 54.
[68] BVerfGE 32, 54 (77 Rn. 66).
[69] BVerwG, Urteil vom 5. November 1987 – 3 C 52/85 –, BVerwGE 78, 251-257, Rn. 22.

Datenerhebungen aus Betriebs- und Geschäftsräumen ohne einschränkende Voraussetzungen erlauben.[70] Das ist mit der Schrankendogmatik des Art. 13 GG nicht vereinbar.

5. Datenerhebung durch Personen, deren Zusammenarbeit mit der Polizei Dritten nicht bekannt ist, und durch Verdeckte Ermittler (§ 25c)

Auch der Einsatz von V-Leuten und Verdeckten Ermittler*innen kann sehr eingriffsintensiv sei. Durch die Maßnahme kann eine vermeintliche Vertrauensbeziehung aufgebaut und dann ausgenutzt werden. Zudem werden oft sehr private Informationen offenbart.[71]

Soweit § 25c Abs. 1 Satz 1 auf die Voraussetzungen des § 25 Abs. 1 Satz 1 Nr. 1 und 2 verweist, wird die Norm dem hohen Eingriffsgewicht nicht gerecht.[72]

6. Datenerhebung durch Telekommunikationsüberwachung (§ 26)

Die Befugnis zur Telekommunikationsüberwachung in § 26 wird ausgeweitet. Das ist abzulehnen und mit Grundrechten teilweise nicht vereinbar.

Eine wie vorliegend mindestens schwerwiegende heimliche Überwachung der Telekommunikation ist gerade dann, wenn die Eingriffsschwelle wie in § 26 Abs. 1 Satz 1 Nr. 2 und 3 ins Vorfeld einer konkreten Gefahr verlagert wird, nur zum Schutz oder zur Bewehrung von besonders gewichtigen (hochrangigen) Rechtsgütern zulässig.[73] Dem entspricht jedenfalls eine Begrenzung auf besonders schwere Straftaten im verfassungsrechtlichen Sinn, also zunächst solche, die mit einer Höchstfreiheitsstrafe von mehr als fünf Jahren bedroht sind.[74]

Die Tatbestände in § 26 Abs. 1 Satz 1 Nr. 1 und 2 werden dem nicht durchgängig gerecht. Zu kritisieren ist insbesondere dynamische Verweisung auf § 100a Abs. 2 StPO, der auch weniger schwere Straftaten und Vorfelddelikte umfasst.[75]

7. Quellen-Telekommunikationsüberwachung und Online-Durchsuchung (§§ 26a, 26b)

Mit § 26a wird die Quellen-Telekommunikationsüberwachung eingeführt. Die Bezeichnung als „Telekommunikationsüberwachung informationstechnischer Systeme" ist irreführend. Es geht um die Infiltration informationstechnischer Systeme mit Hilfe von Spähsoftware (Staatstrojaner) zum Zwecke der Telekommunikationsüberwachung. Bei der Online-Durchsuchung nach § 26b wird ebenfalls ein Staatstrojaner eingesetzt. Dieser kann grundsätzlich auf sämtliche Daten auf dem informationstechnischen System zugreifen.

---

[70] Gesetzentwurf, S. 185.
[71] BVerfG, Beschluss des Ersten Senats vom 17. Juli 2024 - 1 BvR 2133/22 -, Rn. 184.
[72] Siehe oben II.2.
[73] BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025 - 1 BvR 2466/19 -, Rn. 132.
[74] BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025 - 1 BvR 2466/19 -, Rn. 137.
[75] Siehe oben II.1.a. und b.cc.

Beide Befugnisse sind erheblichen Bedenken ausgesetzt. Sie greifen tief in Grundrechte ein, ohne durchgehend gehaltvollen Voraussetzungen zu unterliegen (**dazu unter a.**). Die Anforderungen an die genutzte Software werden nicht unabhängig überprüft (**dazu unter b.**) und die IT-Sicherheit wird gefährdet, indem ein Anreiz gesetzt wird IT-Schwachstellen offen zu halten (**dazu unter c.**).

a. Unverhältnismäßiger Eingriff in das IT-Grundrecht

Sowohl die Quellen-Telekommunikationsüberwachung als auch die Online-Überwachung greifen in das **Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme** (IT-Grundrecht) ein.[76]

Das Eingriffsgewicht der Quellen-Telekommunikationsüberwachung ist insbesondere höher als bei der „normalen Telekommunikationsüberwachung", wie das Bundesverfassungsgericht jüngst dargelegt hat:

> „Angesichts der ubiquitären und vielfältigen Nutzung von IT-Systemen findet inzwischen auch zunehmend jede Art individuellen Handelns und zwischenmenschlicher Kommunikation in elektronischen Signalen ihren Niederschlag und wird so insbesondere der Quellen-Telekommunikationsüberwachung zugänglich. Die Überwachung erfasst damit auch tief in den Alltag hineinreichende, auch höchst private und spontane Kommunikationsvorgänge einschließlich gespeicherter Bilder und Dokumente. Erfasst werden letztlich alle über das Internet transportierten Daten, so etwa das Nutzerverhalten im World Wide Web und die hierbei zum Ausdruck kommenden Interessen, Wünsche und Vorlieben (vgl. auch BVerfGE 154, 152 <243 Rn. 151>). [...]
>
> Eingriffsverstärkend wirkt auch, dass eine Quellen-Telekommunikationsüberwachung nicht nur heimlich erfolgt, sondern mit dem Zugriff auf ein IT-System gezielt Sicherungsmechanismen wie insbesondere der Einsatz von Verschlüsselungstechnologie umgangen werden. Die Vereitelung solchen informationellen Selbstschutzes erhöht das Gewicht der Grundrechtseingriffe (vgl. insoweit BVerfGE 120, 274 <324 f.>). Mit dem Zugriff auf das IT-System werden zudem berechtigte Erwartungen in dessen Integrität und Vertraulichkeit beeinträchtigt. Verbunden ist damit ein hohes Gefährdungspotential. Einmal in das IT-System eingedrungen, ist die entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems überwunden (vgl. auch BVerfGE 120, 274 <314>)."[77]

[76] BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025 - 1 BvR 2466/19 -, Rn. 85 ff.
[77] BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025 - 1 BvR 180/23 -, Rn. 188 ff.

Der Eingriff ist bei der Online-Durchsuchung, bei der nicht nur auf Kommunikationsdaten zugegriffen wird, nochmal gesteigert.

Beide Methoden sind daher abzulehnen. Jedenfalls muss ihr Einsatz an hinreichend gehaltvolle Voraussetzungen geknüpft werden. Dem wird § 26a nicht gerecht. Zu kritisieren ist insbesondere der dynamische Verweis auf den Straftatenkatalog des § 100b Abs. 2 StPO, der auch weniger schwere Straftaten und Vorfelddelikte umfasst.[78] Unverhältnismäßig ist auch die Adressat*innenregelung in § 26a Abs. 1 Nr. 3 Buchst. b. Da bei der Quellen-Telekommunikationsüberwachung und der Online-Durchsuchung informationstechnische Systeme infiltriert werden, kann es auf die Nutzung des Telekommunikationsanschlusses nicht ankommen.

§ 26b Abs. 2 enthält zwar eine eigene Regelung zur Überwachung von Dritten, aber § 26b Abs. 1 verweist umfassend auf § 26a Abs. 1. Hier sollte eine Klarstellung erfolgen, dass nicht auf § 26a Abs. 1 Nr. 3 verwiesen wird, denn dies wäre verfassungswidrig.[79]

b. Fehlende Überprüfung der rechtlichen Anforderungen an die genutzte Software

§ 26a Abs. 2 und § 26b Abs. 9 sehen verschiedene Anforderungen an die genutzte Software vor. Zudem sind bei der Online-Durchsuchung nach § 27a Abs. 2 Satz 2 technische Vorkehrungen gegen die Erhebung Daten aus dem Kernbereich privater Lebensgestaltung zu treffen.[80]

Diese technischen Anforderungen entsprechen der Rechtsprechung des Verfassungsgerichts. Sie werden jedoch nicht verfahrensrechtlich abgesichert.

Das nach § 26 Abs. 2 und § 36b Abs. 6 anordnende Gericht hat zwar die Rechtmäßigkeit der Maßnahme zu überprüfen. Es spricht einiges dafür, dass hierzu auch die Überprüfung der oben genannten Anforderungen gehört. Für eine solche Überprüfung ist das Gericht aber nicht ausgestattet, sodass es sich bestenfalls auf die Angaben der Polizei verlässt. Dies führt im Ergebnis dazu, dass die Polizei beliebige Staatstrojaner nach Gutdünken einsetzten kann, sofern ein Beschluss über eine Maßnahme einmal erlangt werden kann.

Aus der Perspektive des IT-Grundrechts ist ein derart **blindes Vertrauen in die von der Polizei einzusetzenden Staatstrojaner** ohne einen rechtsstaatlich ausreichenden Überprüfungsmechanismus nicht hinnehmbar. Es kommt erschwerend hinzu, dass die einzusetzende Software auch von einem externen Anbieter stammen kann, sodass die Polizei mitunter selbst nicht mit Sicherheit einzuschätzen vermag, welche Funktionen die einzusetzende Software ausführt. Diese enthalten oftmals zusätzliche, in Deutschland verfassungsrechtlich

[78] Siehe oben II.1.a. und b.cc.
[79] BVerfGE 141, 220 (Rn. 115).
[80] Vgl. dazu BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025 - 1 BvR 180/23 -, Rn. 262.

schlechthin nicht zugelassene Funktionen, etwa zur bewussten Manipulation des Zielsystems durch Unterschieben von Beweismitteln, die dann bei einer offenen Durchsuchung aufgefunden werden können. Die Problematik zeigt sich beispielhaft am Einsatz der **Pegasus-Software** durch das Bundeskriminalamt. Pegasus ist eine Spähsoftware, die von dem israelischen Unternehmen „NSO Group" zum Ausspähen von iOS- und Android-Geräten entwickelt wurde. Die Software kann ohne physischen Zugriff auf den Endgeräten installiert werden und anschließend unbemerkt auf sämtliche Daten zugreifen, inklusive verschlüsselter Chats. Darüber hinaus ist die Software in der Lage, unbemerkt Kamera und Mikrofon des Geräts anzuschalten.[81] Ob eine modifizierte Version den Anforderungen des deutschen Recht genügen würde, müsste mindestens unabhängig überprüft werden.

Entsprechend hat das Bundesverfassungsgericht jüngst hervorgehoben, dass das Gefährdungspotential von Staatstrojanern besonders ausgeprägt ist, wenn sich Behörden privater Dritter bedienen, um die Infiltration zu vollziehen.[82] Der Entwurf nimmt billigend in Kauf, dass auch in Berlin Staatstrojaner zum Einsatz kommen, die gerade nicht den (ohnehin nur fragmentarischen) gesetzlichen Anforderungen an deren technische Gestaltung genügen.

c. Fehlendes Schwachstellenmanagement

Darüber hinaus fehlt es nach wie vor an einem **Schwachstellenmanagement** hinsichtlich des Einsatzes von Staatstrojanern. Um Staatstrojaner in die jeweiligen Systeme einzuschleusen, werden unter anderem IT-Sicherheitslücken ausgenutzt. Deshalb haben Behörden ein Interesse daran, die Sicherheitslücken nicht bei den Hersteller*innen zu melden, sondern sie offen zu halten. Dem steht entgegen, dass das IT-Grundrecht den Staat dazu verpflichtet, zum Schutz der Systeme vor Angriffen durch Dritte beizutragen.[83] Diese **Schutzpflicht** verpflichtet den Gesetzgeber, den Umgang der Behörden mit Sicherheitslücken, die den Herstellern nicht bekannt sind, zu regeln.[84]

Der Entwurf weitet den Einsatz von Staatstrojanern unter Ausnutzung von Sicherheitslücken aus, ohne dass bisher ein Schwachstellenmanagement etabliert wurde. Dass ein solches Schwachstellenmanagement unbedingt erforderlich ist, hat das Bundesverfassungsgericht bereits deutlich gemacht:

---

[81] Amnesty International, Forensic Methodology Report – How To Catch NSO Group's Pegasus, 2021, abrufbar unter https://www.amnesty.org/en/documents/doc10/4487/2021/en/; Untersuchungsausschuss zum Einsatz von Pegasus und ähnlicher Überwachungs- und Spähsoftware, Bericht über die Prüfung von behaupteten Verstößen gegen das Unionsrecht und Missständen bei der Anwendung desselben im Zusammenhang mit dem Einsatz von Pegasus und ähnlicher Überwachungs- und Spähsoftware v. 22.05.2023 (2022/2077(INI)), abrufbar unter https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_DE.html.

[82] BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025 - 1 BvR 2466/19 -, Rn. 114.

[83] BVerfG, Beschluss des Ersten Senats vom 08. Juni 2021, 1 BvR 2771/18, Ls. 2 lit. b.

[84] BVerfG, Beschluss des Ersten Senats vom 08. Juni 2021, 1 BvR 2771/18, Rn. 41.

> „Die grundrechtliche Schutzpflicht des Staates verlangt auch eine Regelung zur grundrechtskonformen Auflösung des Zielkonflikts zwischen dem Schutz informationstechnischer Systeme vor Angriffen Dritter mittels unbekannter Sicherheitslücken einerseits und der Offenhaltung solcher Lücken zur Ermöglichung einer der Gefahrenabwehr dienenden Quellen-Telekommunikationsüberwachung andererseits."[85]

Die Ausnutzung von staatlicherseits geheim gehaltenen Sicherheitslücken ist durchaus keine düstere Fantasie, sondern bittere Realität. Erinnert sei an den Vorfall um „**WannaCry**" vom 12. Mai 2017: Innerhalb weniger Stunden infiltrierte dieses Schadprogramm, ein sogenannter Kryptotrojaner, weltweit etwa 220.000 Systeme. Der Trojaner verschlüsselte die Daten auf den betroffenen Computern und bot den Nutzern zeitgleich einen Code für die Entschlüsselung an, ansonsten werde die Löschung der Daten veranlasst. In Deutschland war davon beispielsweise die Deutsche Bahn betroffen. Besonders schwer traf es das Gesundheitssystem in Großbritannien. Zahlreiche Rechner des National Health Service waren befallen. Patient*innen berichteten von chaotischen Zuständen. Die Daten von Krebs- und Herzpatient*innen standen nicht mehr zur Verfügung. Viele Kranke mussten in andere Kliniken umgeleitet werden.

Der WannaCry-Trojaner nutzte eine Lücke im Betriebssystem Microsoft Windows. Diese Lücke war schon Jahre zuvor von der National Security Agency, des auf Hacking spezialisierten US-Geheimdienstes, entdeckt, aber nicht an den Hersteller Microsoft gemeldet worden, damit er die Sicherheitslücke schließe. Brad Smith, Präsident von Microsoft, erhob in einer Erklärung den Vorwurf, die Geheimdienste würden diese Lücken absichtsvoll horten, statt sie sofort an die Hersteller zu melden.

Die Problematik verschärft sich, wenn private Unternehmen hinzugezogen werden. Hierzu sei wieder beispielhaft auf den **Pegasus-Trojaner** hingewiesen, der Medienberichten zufolge vom Bundeskriminalamt genutzt wird. Es ist davon auszugehen, dass die ausgenutzten Sicherheitslücken dem Bundeskriminalamt gar nicht bekannt sind, weil die NSO Group die Kenntnisse als Betriebsgeheimnisse für sich behält. Sie können daher auch im Auftrag von autokratischen Staaten ausgenutzt werden, um Journalist*innen, Menschenrechtler*innen, Rechtsanwält*innen und Oppositionelle sowie ausländischen Politiker*innen und Diplomat*innen auszuspähen. Die Schäden für die Demokratie sind gravierend. Für Einzelne können die Folgen unter Umständen tödlich sein. So wird beispielsweise vermutet, dass die mittels Pegasus erfolgte Überwachung verschiedener Personen im Zusammenhang mit der Ermordung des saudischen Journalisten Jamal Khashoggi im Herbst 2018 stand.[86]

---

[85] BVerfG, Beschluss des Ersten Senats vom 08. Juni 2021, 1 BvR 2771/18, Ls. 2 lit. b.
[86] Zeit vom 18. Juli 2021, https://www.zeit.de/politik/ausland/2021-07/jamal-khashoggi-mord-journalist-ueberwachung-software-pegasus-saudi-arabien.

8. Nachträglicher biometrischer Abgleich mit öffentlich zugänglichen Daten aus dem Internet (§ 28a)

§ 28a sieht die Befugnis vor, biometrische Daten zu Gesichtern und Stimmen mit öffentlich zugänglichen personenbezogenen Daten aus dem Internet abzugleichen.

Diese Befugnis sieht sich rechtlichen Bedenken ausgesetzt. Der Aufbau einer biometrischen Referenzdatenbank auf Vorrat wäre verfassungs- und unionsrechtswidrig (**dazu unter a.**). Ein Rückgriff auf kommerzielle Anbieter wäre unzulässig (**dazu unter b.**). Unabhängig davon genügen die Voraussetzungen des Abgleichs nicht den verfassungsrechtlichen Anforderungen (**dazu unter d.**).

a. Aufbau einer biometrischen Referenzdatenbank auf Vorrat wäre rechtswidrig

§ 28a enthält keine Vorgaben für **die technische Umsetzung des Abgleichs**. Nach § 28 Abs. 1 Satz 3 dürfen allgemein öffentlich zugängliche personenbezogene Daten aus dem Internet zum Zwecke des Abgleichs erhoben, gespeichert und aufbereitet werden. Eine Regelung zur Löschung der Daten nach Durchführung des Abgleichs wie in § 15b Abs. 4 AsylG fehlt.

Das legt nahe, dass den Behörden mittelbar auch die Befugnis eingeräumt werden soll, **biometrische Referenzdatenbanken auf Vorrat** aufzubauen. Auch aus technischer Sicht wäre es nicht praktikabel, vor jeder einzelnen Abgleichmaßnahme den Datenbestand im Internet erneut auszulesen. Dies würde schlichtweg sehr lange dauern. Eine methoden- und technikneutrale Ausgestaltung von Gesetzen mag im Grundsatz zwar zulässig sein und kann sich im Allgemeinen als durchaus sinnvoll erweisen. Etwas anderes ergibt sich aber dann, wenn – wie vorliegend – die technische Komponente wesentlich ist, um die Grundrechtsrelevanz der Befugnis zu beurteilen. Da der Aufbau einer Datenbank das Eingriffsgewicht der Befugnis maßgeblich erhöhen würde, würde schon der Vorbehalt des Gesetzes erfordern, dass dies hinreichend bestimmt und normenklar im Gesetzestext verankert würde. Eine Regelung in der Verwaltungsvorschrift nach § 29a Abs. 5 genügt nicht.

Davon abgesehen, wäre der Aufbau einer biometrischen Referenzdatenbank auf Vorrat mit ungezielt ausgelesenen Daten aus dem Internet aber ohnehin unionsrechts- und verfassungswidrig.

Europarechtlich ist der Einsatz von KI-Systemen zur biometrischen Fernidentifikation insbesondere an den Vorgaben der Verordnung (EU) 2024/1689 (KI-VO) zu messen. Ein biometrischer Abgleich ohne KI-System wäre fernliegend. Aus jedem Bild muss zunächst ein biometrisches Template extrahiert, also die biometrischen Daten ausgelesen werden, bevor ein

Treffer oder Nichttreffer festgestellt werden kann.[87] Gleiches gilt für Stimmmuster. Auch der Entwurf geht offenbar davon aus, dass ein KI-System zum Einsatz kommt.[88] Die KI-Verordnung ist somit anwendbar, zumal die Ausnahme der nationalen Sicherheit in Art. 2 Abs. 3 KI-VO jedenfalls für den Großteil des Anwendungsbereichs nicht einschlägig ist. Der Begriff knüpft an die Kompetenzverteilung zwischen Union und Mitgliedsstaaten in Art. 4 Abs. 2 Satz 2 und Satz 3 EUV an und wird vom EuGH sehr eng ausgelegt.[89] Zwar benennt der EuGH als Beispiel terroristische Aktivitäten, sodass – ausschließlich – bei der Abwehr terroristischer Gefahren die Ausnahme zumindest teilweise greifen könnte. Da allerdings auch die Europäische Union im Bereich der Terrorismusbekämpfung Kompetenzen hat[90] kann auch im Bereich der Terrorabwehr nicht pauschal auf die nationale Sicherheit verwiesen werden.[91]

Art. 5 Abs. 1 lit. e KI-VO verbietet insbesondere die Verwendung von KI-Systemen, die Datenbanken zur Gesichtserkennung durch das ungezielte Auslesen von Gesichtsbildern aus dem Internet erstellen oder erweitern. Ein **ungezieltes Auslesen von Gesichtsbildern** wäre unionsrechtlich demnach nur möglich, wenn damit kein Datenbankaufbau verbunden ist. Ungezielt ist das Auslesen immer dann, wenn – wie die Befugnisse es vorliegend erlauben – nicht gezielt nur einzelne Bilder ausgesucht und abgeglichen werden sollen.

Auch verfassungsrechtlich würde der Aufbau einer umfassenden biometrischen Referenzdatenbank – bestehend aus allen öffentlich zugänglichen Lichtbildern, Videos und Tonaufnahmen aus dem Internet – **unverhältnismäßig in Grundrechte eingreifen**. Das Bundesverfassungsgericht hat mehrfach herausgestellt, dass biometrische Daten besonders schutzwürdig sind.[92] Durch den Aufbau einer Datenbank, um biometrische Daten vorzuhalten, wären überwiegend Grundrechte von Millionen, wenn nicht Milliarden von unbeteiligten Personen betroffen, die keinen Anlass für polizeiliche Überwachung gegeben haben. Die Streubreite wäre dadurch enorm. Mit dem Aufbau einer solchen Datenbank ginge ein erhebliches Missbrauchsrisiko einher. Sicherheitsbehörden könnten jederzeit jede Person identifizieren, im digitalen genauso wie im analogen Raum. Damit wäre der Grundstein gelegt, um von allen Menschen umfassende

---

[87] European Data Protection Board (EDPB) Guidelines on the use of facial recognition technology in the area of law enforcement, 26.04.2023, S. 9.
[88] Gesetzentwurf, S. 237 und 240.
[89] EuGH NJW 2021, 531 (538); NVwZ 2022, NVWZ 2022, 1697 (1703); auch Erwägungsgrund 24 stellt dem Zweck nationalen Sicherheit nach Art. 4 Abs. 2 EUV die Zwecke der Strafverfolgung oder öffentlichen Sicherheit gegenüber, sodass diese Zwecke jedenfalls nicht unter die nationale Sicherheit gefasst werden können.
[90] Siehe Richtlinie (EU) 2017/541.
[91] vgl. für die entsprechende Ausnahme in der DSGVO *Bäcker*, in: BeckOK DatenschutzR, 49. Ed. 1.8.2023, DS-GVO Art. 2 Rn. 9b.
[92] BVerfG, Beschluss vom 18. Dezember 2018, 1 BvR 142/15, Rn. 53: „höchstpersönliche Merkmale wie das Gesicht"; vgl. auch BVerfG, Urteile des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19 und 1 BvR 2634/20, Rn. 87

Bewegungs- und Persönlichkeitsprofile zu erstellen. Hinzu kämen erhebliche Sicherheitsrisiken, da biometrische Daten oft als Authentifizierungsinstrument genutzt werden und unveränderlich sind.

b. Nutzung kommerzieller biometrischer Datenbanken wäre rechtswidrig

Anlass für die Einfügung des § 28a ist laut Entwurfsbegründung der Fall von **Daniela Klette**. Diese wurde von Journalist*innen mit Hilfe des kommerziellen Anbieters PimEyes aufgespürt. Anbieter wie PimEyes verstoßen sowohl gegen das Scraping-Verbot der KI-Verordnung (s.o.) als auch gegen Datenschutzrecht. Beispielweise hat der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg ein Bußgeldverfahren eröffnet.[93]

Der Gesetzentwurf verhält sich nicht ausdrücklich zu der Frage, ob die Polizei solche **kommerziellen Datenbanken** nutzen könnte. § 28a Abs. 4 Satz 3 erlaubt die Inanspruchnahme von Auftragsverarbeitenden unter bestimmten Voraussetzungen. Diese müssen zwar ihren Sitz in einem Mitgliedstaat der Europäischen Union oder in einem Schengen-assoziierten Staat haben, was eine Auftragsverarbeitung durch PimEyes ausschließt. Anderer private Anbieter könnten jedoch grundsätzlich herangezogen werden.

Ein Rückgriff auf rechtswidrige Angebote Privater ist für den Staat aber ausgeschlossen. Selbst wenn kommerzielle Datenbanken legal erstellt würden, dürfte der Staat die für ihn geltenden rechtlichen Grenzen nicht umgehen, indem er auf diese Anbieter zurückgreift.

c. Unverhältnismäßigkeit des Abgleichs

Aber selbst wenn kein Bild- und Stimmmaterial vorab ausgelesen und in einer Datenbank bevorratet würde, stellt auch der Abgleich an sich einen **schwerwiegenden Eingriff in das Recht auf informationelle Selbstbestimmung** dar.

Auch dann ist die Streubreite immens. Denn auch Nicht-Treffer stellen Eingriffe in die Grundrechte der Personen dar, deren Daten abgeglichen werden.[94] Da einzelne Personen nur begrenzt beeinflussen können, ob Bild- und Videomaterial von ihnen gegen ihren Willen im Internet veröffentlicht wird, sind davon potenziell alle Menschen betroffen. Außerdem können Rückschlüsse auf besonders sensible Daten wie politische Einstellungen und sexuelle Orientierung gezogen werden (z.B. bei Aufnahmen von Demonstrationen, Parteiveranstaltungen, Gottesdiensten etc.). Anonymität im Internet, das einen erheblichen Teil des öffentlichen Raumes darstellt, wird damit faktisch unmöglich gemacht. Das ist mit enormen Abschreckungseffekten verbunden und hat erhebliche Auswirkungen auf die Ausübung von Grundrechten. Insbesondere die Ausübung der Meinungsfreiheit über öffentliche Profile in Sozialen Medien wird damit besonders beeinträchtigt. Die Systeme zum biometrischen Abgleich sind darüber hinaus höchst

[93] https://www.baden-wuerttemberg.datenschutz.de/pimeyes-lfdi-eroeffnet-bussgeldverfahren/.
[94] BVerfG, Beschluss des Ersten Senats vom 18. Dezember 2018, 1 BvR 142/15, Rn. 51.

fehleranfällig und potentiell diskriminierend. Eingriffsintensivierend wirkt zudem, dass die Abgleiche heimlich stattfinden und Rechtsschutzmöglichkeiten damit erheblich beschränkt sind.

Immerhin sollen nach § 28a Abs. 2 Satz 2 Echtzeit-Abgleiche jedenfalls teilweise, nämlich für Echtzeit-Lichtbild- und Echtzeit-Videodateien ausgeschlossen sein. Für Stimmen fehlt ein entsprechender Ausschluss bisher. Art. 5 Abs. 1 lit. h KI-VO erlaubt den Echtzeit-Abgleich nur in engen Grenzen.

Wegen des hohen Eingriffsgewichts sind die Befugnisse zum biometrischen Abgleich abzulehnen. Jedenfalls müssen sie an **strenge Voraussetzungen** geknüpft werden. Dem wird der Entwurf nicht gerecht.

§ 28a Abs. 1 Nr. 1 setzt zwar grundsätzlich eine (konkrete) Gefahr für besonders gewichtige Rechtsgüter voraus. Die genannten Rechtsgüter bedürfen teilweise der Einschränkung und Konkretisierung.[95] Zudem fehlt es an einer hinreichend bestimmten Adressat*innenregel. § 28a Abs. 1 Nr. 1 verlangt zwar, dass die Maßnahme zur Identifizierung oder Ermittlung des Aufenthaltsorts der nach den §§ 13 oder 14 verantwortlichen Person erforderlich ist. Dies schließt jedoch nicht aus, dass auch die biometrischen Daten anderer Personen (z.B. Kontaktpersonen) gezielt abgeglichen werden.

§ 28a Abs. 1 Nr. 2 verweist auf § 100b StPO, was verschiedene verfassungsrechtliche Probleme mit sich bringt.[96] Zudem ist sind nicht beide Bedingungen der konkretisierten Gefahr abgebildet.[97]

§ 28a Abs. 1 Nr. 3 enthält zwar eine Beschränkung auf terroristische Straftaten, es wird jedoch nicht klargestellt, dass nur die Daten der dort genannte Person abgeglichen werden dürfen.

Zudem fehlt es an weiteren **Schutzvorkehrungen** unter anderem gegen Diskriminierung. Zudem fehlt es an einer auf die Maßnahme zugeschnittenen Vorschrift zum Schutz des Kernbereichs privater Lebensgestaltung. Im Internet kursiert eine Vielzahl sensibler Aufnahmen, die oftmals auch ohne Einverständnis der abgebildeten Personen erstellt und veröffentlicht werden. Deren Verarbeitung sollte ausgeschlossen werden.[98]

9. Automatisierte Anwendung zur Analyse vorhandener Daten (§ 47a)

§ 47a schafft eine Rechtsgrundlage für **automatisierte Datenanalysen** zur Gefahrenabwehr und Verhütung von Straftaten in drei verschiedenen Tatbestandsvarianten (§ 47a Abs. 1 Satz 2 Nr. 1 bis 3).

---

[95] Siehe oben II.1.a.
[96] Siehe oben II.1.a. und b.cc.
[97] Siehe oben II.1.b.aa.
[98] Vgl. § 15b Abs. 2 AsylG.

Polizeiliche Datenanalysen stellen auch bei verfassungskonformer gesetzlicher Ausgestaltung erhebliche Grundrechtseingriffe dar. Die Analyse enormer Mengen polizeilicher Daten aus verschiedenen Datenbanken mit komplexen Algorithmen führt zu nicht nachvollziehbaren Analyseergebnissen. Die Analysen erfolgen heimlich ohne Kenntnis der Betroffenen. Es besteht die Gefahr, dass durch Fehler und diskriminierende Analysevorgänge auch Personen in polizeilichen Fokus geraten, die dafür keinen Anlass geboten haben. Gleichzeitig ist die Effizienz und Wirksamkeit polizeilicher Datenanalysen zur Gefahrenabwehr bislang nicht nachgewiesen. Aus diesem Grunde ist die Schaffung von Rechtsgrundlagen für methodenoffene Analysen und automatisierte Erkenntnisgewinne insgesamt kritisch zu sehen.

Der vorliegende Entwurf orientiert sich erkennbar an den Maßstäben des Bundesverfassungsgerichts aus der Entscheidung vom 16. Februar 2023,[99] setzt diese jedoch nicht hinreichend um.

Bei der vorgesehenen Datenanalyse aller Tatbestandsvarianten handelt es sich um einen **schwerwiegenden Grundrechtseingriff**, da weder **Art und Umfang der Daten** noch Analysemethode durch den Gesetzesentwurf ausreichend beschränkt sind, um das Eingriffsgewicht maßgeblich zu reduzieren. Insbesondere werden nach § 47a Abs. 2 des Entwurfs in die Analyse mit Vorgangs-, Fall- und Telekommunikationsdaten sowie Daten aus Asservaten große Mengen von Daten von unbeteiligten Menschen einbezogen, die keinen Anlass für polizeiliche Maßnahmen gegeben haben, insbesondere Betroffene und Zeug*innen von Straftaten sowie Kontaktpersonen. § 47a Abs. 2 Satz 5 ASOG-E des Entwurfs schränkt das Eingriffsgewicht nicht ein, da in der polizeilichen Praxis keine Trennung von Vorgangsdaten Unbeteiligter und Beteiligter erfolgt und daher ein verlässlicher Ausschluss nicht möglich ist. Zudem können über § 47a Abs. 2 Satz 2 und 4 des Entwurfs unbegrenzt weitere Daten in die Analyse eingeführt werden, insbesondere auch einzelne Daten aus dem Internet.

Auch ist die **Analysemethode** nur geringfügig eingeschränkt und ermöglicht den Einsatz von hochkomplexen Algorithmen und künstlicher Intelligenz, was sich eingriffserschwerend auswirkt.[100] Der Entwurf gestattet weitgehende Analysen, die über einen bloßen Datenabgleich erheblich hinausgehen. § 47a Abs. 1 Satz 6 StGB schließt den Einsatz von Analysetools zur Ermittlung von polizeilichen Entscheidungsgrundlagen nicht aus. Im Entwurf fehlen zudem hinreichende tatsächliche Vorkehrungen gegen Diskriminierung und zur Erkennung und Vermeidung von Fehlern.[101]

---

[99] BVerfG, Urteil des Ersten Senats vom 16. Februar 2023 - 1 BvR 1547/19.
[100] BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 100.
[101] BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 109.

Aufgrund dessen genügt § 47a Abs. 1 Satz Nr. 2 des Entwurfs nicht den verfassungsrechtlichen Anforderungen, weil die Norm eine dynamische Verweisung auf den unzureichenden Straftatenkatalog des § 100a Abs. 2 StPO enthält, der auch Vorfelddelikte einschließt, und nicht die zweite Bedingung der konkretisierten Gefahr umsetzt.[102]

Weiterhin ist die Einhaltung der Grundsätze der Zweckbindung und Zweckänderung nicht ausreichend sichergestellt. Da die Daten für die Analyse dauerhaft zusammengeführt werden, bedarf es einer Sicherung der Zweckbindung durch eine umfassende **Kennzeichnung**.[103] Zwar wird in § 47a Abs. 2 Satz 6 auch § 42b und damit die Kennzeichnungspflicht in Bezug genommen, jedoch auch dessen Ausnahmen in Absatz 3. Stattdessen müsste sichergestellt sein, dass nur gekennzeichnete Daten in die Analyse einfließen können. Zudem überlässt der Gesetzgeber die Entscheidung über die einzubeziehenden personenbezogenen Daten in § 47a Abs. 2 der Verwaltung, anstatt die grundrechtssensiblen Leitentscheidungen selbst zu treffen.

Positiv ist zu bemerken, dass der Gesetzgeber sowohl **Kontrollen** des*r behördlichen Datenschutzbeauftragten (§ 47a Abs. 3 Satz 5), der Landesdatenschutzbeauftragten (§ 51b Satz 1 Nr. 1) sowie eine parlamentarische Kontrolle (§ 47a Abs. 7 des Entwurfs) vorgesehen ist. Jedoch müssen Inhalt und Umfang der Kontrollen für die besondere Maßnahme der Datenanalyse gesetzlich näher konkretisiert werden. Gerade zu Beginn der Nutzung der operativen und strategischen Datenanalyse ist eine externe Kontrolle zum Ausschluss von Fehlern, Diskriminierung und Missbrauch in geringeren Abständen notwendig. Nur durch regelmäßige umfassende und verdachtsunabhängige Kontrollen kann der eingeschränkte Individualrechtsschutz bei der ohne Wissen der Betroffenen erfolgenden Datenanalyse ausgeglichen werden.

Der Entwurf genügt insgesamt dem Gesetzesvorbehalt und dem Wesentlichkeitsgrundsatz sowie den Anforderungen an Bestimmtheit und Normenklarheit nicht, da für grundrechtswesentliche Bereiche die durch den Gesetzgeber vorzunehmenden Abwägungen an die Verwaltung durch Verwaltungsvorschriften ausgelagert werden. Insbesondere fehlt es in § 47a an expliziten **Vorkehrungen gegen eine unangemessen verzerrende und diskriminierende Wirkung** der Datenauswahl und -analyse, gerade für den Einsatz von künstlicher Intelligenz. Darüber hinaus bedarf es gerade auch gesetzlicher Regelungen zur praktischen Durchführung und Wirksamkeit der technisch-organisatorischen Vorgaben für Kontrollen und zur Sicherung des Grundsatzes der Zweckbindung sowie zur Vermeidung und Erkennung von Fehlern und Diskriminierung.

---

[102] Näher dazu oben II.1.a.und b.aa. und cc.

[103] BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 65.

Über den konkreten Entwurf hinaus sollte bei Ausführung der im Entwurf vorgesehenen Datenanalysen nicht auf **Software privater Anbieter*innen wie zum Beispiel Palantir**, sondern auf staatliche und unternehmensunabhängige Software zurückgegriffen werden. Zwar ist der Einsatz privater Software im Rahmen staatlicher Datenverarbeitung nicht per se ausgeschlossen.[104] Wenn im Bereich der polizeilichen Staatsaufgaben auf Systeme privater Anbieter zurückgegriffen wird, stellt dies eine Auslagerung des Grundrechts- und Datenschutzes vom grundrechtsverpflichteten Staat auf private Unternehmen dar. Dies ist risikoreich, da sensiblen und persönlichkeitsrechtsrelevanten Daten mit Algorithmen analysiert werden, deren Funktionsweise nicht nachvollzogen werden kann. Dies führt zu weniger Transparenz und Schwierigkeiten bei der Kontrolle. Manipulation und mögliche Hintertüren und damit das Risiko von Leaks von und unbefugtem Zugriff auf polizeiliche Daten können nie, auch nicht durch vertragliche Vereinbarungen vollständig ausgeschlossen werden. Dies gilt auch, wenn private Software ohne Verbindung zum Internet und auf staatlichen Servern eingesetzt und betrieben wird. Bei Wartung und Fehlerkorrektur besteht ein Risiko, dass Private Zugriff auf Datensätze und Analyseergebnisse erhalten, gerade, wenn zur Wartung Personal des privaten Unternehmens innerhalb der polizeilichen Infrastruktur mit Zugang zu den polizeilichen Servern eingesetzt wird.[105] Gleichzeitig ist unklar, wie eine Aktualität der dauerhaft zusammengeführten Datensätze im Analysesystem und eine jederzeitige Verfügbarkeit des Analysetools sichergestellt werden kann, wenn die Analysesoftware vollständig isoliert von öffentlichen Netzen und damit auch von internen Dienstnetzwerken betrieben werden soll.

Besondere Risiken bestehen beim Einsatz von Software außereuropäischer Anbieter*innen, die mit anderen Regierungen und Geheimdiensten auch autoritärer Staaten zusammenarbeiten und bei denen durch die Rechtslage im Staat ihres Unternehmenssitzes die Gefahr auch ungewollter staatlicher Datenzugriffe besteht.

Ebenso besteht beim Einsatz der Software privater Anbieter*innen die Gefahr, dass Algorithmen und Ergebnisse intransparent verbleiben und so Fehler und insbesondere diskriminierende und verzerrende Algorithmen schlechter identifiziert und beseitigt werden können. Dies gilt umso mehr, wenn hochkomplexe Analysen mittels künstlicher Intelligenz erfolgen.[106]

Auch ist die Lizensierung einer privaten Software mit erheblichen Kosten verbunden.[107] Dies gilt umso mehr, wenn Anbieter*innen bei deutschen Behörden eine weitgehende Monopolstellung

---

[104] BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 100.
[105] SZ vom 19. Juni 2025, abrufbar unter https://www.sueddeutsche.de/projekte/artikel/politik/palantir-sicherheit-polizei-thiel-innenminister-e406093/.
[106] BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 100.
[107] In Nordrhein-Westfalen fielen für eine auf Palantir Gotham beruhende Software statt ursprünglich geplanten 14 Millionen Euro nun Kosten in Höhe von 39 Millionen Euro an, WDR vom 25. September 2022,

einnehmen. Es drohen starke Abhängigkeiten, in welchen Anbieter*innen die Preise (wie durch Preisbindungsfristen[108]) und Nutzungsbedingungen weitgehend frei diktieren können. Durch die aufgewendeten Kosten und die Einrichtung einer solchen Software drohen Lock-In-Effekte, die einen späteren Wechsel auf andere Angebote wesentlich erschweren. Aus diesem Grunde ist auch ein Einsatz einer solche Software als vermeintliche „Übergangslösung" abzulehnen.

III. Transparenz

Der Verhältnismäßigkeitsgrundsatz stellt auch Anforderungen an Transparenz, individuellen Rechtsschutz und aufsichtliche Kontrolle. Transparenz der Datenerhebung und -verarbeitung soll dazu beitragen, dass Vertrauen und Rechtssicherheit entstehen können und der Umgang mit Daten in einen demokratischen Diskurs eingebunden bleibt. Durch sie soll, soweit möglich, den Betroffenen subjektiver Rechtsschutz ermöglicht und zugleich einer diffusen Bedrohlichkeit geheimer staatlicher Beobachtung entgegengewirkt werden. Je weniger die Gewährleistung subjektiven Rechtsschutzes möglich ist, desto größere Bedeutung erhalten dabei Anforderungen an eine wirksame aufsichtliche Kontrolle und an die Transparenz des Behördenhandelns gegenüber der Öffentlichkeit.[109]

1. Benachrichtigungspflichten (§§ 27d, 27f)

Die Benachrichtigungs- und Berichtspflichten nach § 27d Abs. 1 und § 27f Abs. 1 sollten auf alle verdeckten Datenerhebungs- und weiterverarbeitungsmaßnahmen erstreckt werden.

2. Auskunftsrecht (§ 50)

Der Auskunftsanspruch des Betroffenen über ihn betreffende Datenverarbeitungen ist das grundlegende Datenschutzrecht.[110]

§ 50 enthält zwar ein solches Auskunftsrecht verweist aber über § 43 Abs. 3 BlnDSG auf die bedenklich unbestimmten Ausschlussgründe des § 42 Abs. 2 BlnDSG. Hinzu kommt, dass die Betroffenen nach dem Wortlaut von § 43 Abs. 6 BlnDSG unter Umständen noch nicht einmal darüber informiert werden müssen, dass von einer Auskunft abgesehen wurde. Ein so weitgehender Ausschluss kann zu kafkaesken Situationen führen und ist unverhältnismäßig.

---

abrufbar unter https://www1.wdr.de/nachrichten/landespolitik/nrw-polizei-datenbank-software-palantir-kosten-100.html; in Baden-Württemberg wurden bereits 25 Millionen Euro für einen Fünf-Jahres-Vertrag investiert, SWR vom 24. Juli 2025, abrufbar unter https://www.swr.de/swraktuell/baden-wuerttemberg/palantir-software-hohe-kosten-drohen-100.html.

[108] heise online/dpa vom 27. Juli 2025, abrufbar unter https://www.heise.de/news/Koalitionszoff-um-Palantir-Software-fuer-Polizei-10497840.html.

[109] BVerfGE 141, 220 (282 Rn. 134 f.)

[110] *Worms*, in: Wolff/Brink (Hrsg.), Datenschutzrecht in Bund und Ländern, 2013, § 19 BDSG Rn. 1.

Bisher bezog sich dieser verlängerte Auskunftsausschluss nur auf die Gründe des Absehens (§ 50 Abs. 3 ASOG).

Gesellschaft für Freiheitsrechte e.V.
Boyenstr. 41
10115 Berlin

info@freiheitsrechte.org
Amtsgericht Berlin-Charlottenburg
Registernummer VR 34505 B

GLS Gemeinschaftsbank eG
IBAN · DE 88 4306 0967 1182 9121 00
BIC · GENODEM1GLS