

Dr. Robert Brockhaus | Rechtsanwalt | Partner
Dr. Vivian Kube, LL.M. (EUI, Florenz) | Rechtsanwältin | Partnerin
Dr. Benjamin Lück | Rechtsanwalt | Partner
Hannah Vos | Rechtsanwältin | Partnerin
David Werdermann, LL.M. | Rechtsanwalt | Partner
Mareile Dedekind, LL.M. | Rechtsanwältin | Freie Mitarbeiterin
Sarah Lincoln | Rechtsanwältin | Freie Mitarbeiterin
Dr. Simone Ruf | Rechtsanwältin | Freie Mitarbeiterin
Philipp Schönberger | Rechtsanwalt | Freier Mitarbeiter
Joschka Selinger | Rechtsanwalt | Freier Mitarbeiter



KM8 Rechtsanwältinnen & Rechtsanwälte, Moosdorfstraße 7-9, 12435 Berlin

Verfassungsgerichtshof des Landes Berlin
Eißholzstraße 30-33
10781 Berlin

per beA

KM8 Rechtsanwältinnen &
Rechtsanwälte GbR
Moosdorfstraße 7-9
12435 Berlin
Telefon: +49 (0)30-75438516
Telefax: +49 (0)30-75438517
E-Mail: info@km8.legal
www.km8.legal

Unser Zeichen: 048/26

Berlin, 27. August 2026

Normenkontrollantrag
gemäß Art. 84 Abs. 7 Nr. 2 VvB, § 14 Nr. 4, §§ 43 ff. VerfGHG

der folgenden Abgeordneten der 19. Wahlperiode des Abgeordnetenhauses von
Berlin, sämtlich mit der Anschrift Margot-Friedländer-Platz, 10117 Berlin:

Fraktion Bündnis 90/Die Grünen:

1. Gollaleh Ahmadi,
2. Daniela Billig,
3. Tuba Bozkurt,
4. Marianne Burkert-Eulitz,
5. Vasili Franco,
6. Silke Gebel,
7. Werner Graf,
8. Bahar Haghanipour,
9. Oda Hassepaß,
10. Bettina Jarasch,

11. Dr. Susanna Kahlefeld,
12. Antje Kapek,
13. Taylan Kurt,
14. Louis Krüger,
15. Benedikt Lux,
16. Ario Mirzaie,
17. Laura Neugebauer,
18. Jian Omar,
19. Andreas Otto,
20. Catherina Pieroth,
21. Klara Schedlich,
22. Katrin Schmidberger,
23. André Schulze,
24. Julian Schwarze,
25. Dr. Stefan Taschner,
26. June Tomiak,
27. Dr. Petra Vandrey,
28. Catrin Wahlen,
29. Sebastian Walter,
30. Christoph Wapler,
31. Daniel Wesener,
32. Tonka Wojahn,
33. Stefan Ziller,

Fraktion Die Linke:

- 34. Philipp Bertram,
- 35. Elke Breitenbach,
- 36. Franziska Brychcy,
- 37. Dr. Michael Efler,
- 38. Claudia Engelmann,
- 39. Elif Eralp,
- 40. Anne Helm,
- 41. Regina Kittler,
- 42. Hendrikje Klein,
- 43. Dr. Klaus Lederer,
- 44. Franziska Leschewitz,
- 45. Kristian Ronneburg,
- 46. Carsten Schatz,
- 47. Niklas Schenker,
- 48. Dr. Manuela Schmidt,
- 49. Niklas Schrader,
- 50. Katina Schubert,
- 51. Tobias Schulze,
- 52. Damiano Valgolio,
- 53. Steffen Zillich,

Antragstellende,

Verfahrensbevollmächtigte: KM8 Rechtsanwältinnen & Rechtsanwälte,
Moosdorfstraße 7-9, 12435 Berlin,

gegen: §§ 24, 24a, 24e, 26a, 26b, 28a, 42a i.V.m. 42b Abs. 4 Satz 1, 42d, 47a des
Allgemeinen Sicherheits- und Ordnungsgesetzes in der Fassung vom 11. Oktober 2006,
zuletzt geändert durch Artikel 3 des Gesetzes vom 15.06.2026 (GVBl. S. 488, 492).

Namens und in Vollmacht der Antragstellenden beantrage ich

1. §§ 24, 24a, 24e ASOG für unvereinbar mit Art. 33 VvB und nichtig zu erklären,

§§ 26a, 26b ASOG für unvereinbar mit Art. 7 i.V.m. Art. 6 VvB, Art. 16 VvB sowie
Art. 33 VvB und nichtig zu erklären,

§ 28a ASOG für unvereinbar mit Art. 26 und Art. 33 VvB und nichtig zu erklären,

§ 42a i.V.m. § 42b Abs. 4 Satz 1 ASOG für unvereinbar mit Art. 7 i.V.m. Art. 6
VvB, Art. 16 VvB, Art. 28 Abs. 2 VvB sowie Art. 33 VvB und nichtig zu erklären,

§ 42d ASOG für unvereinbar mit Art. 7 i.V.m. Art. 6 VvB, Art. 16 VvB, Art. 28
Abs. 2 VvB sowie Art. 33 VvB und nichtig zu erklären,

§ 47a ASOG für unvereinbar mit Art. 7 i.V.m. Art. 6 VvB, Art. 16 VvB, Art. 28 Abs.
2 VvB sowie Art. 33 VvB und nichtig zu erklären,

2. anzuordnen, den Antragstellenden die notwendigen Auslagen für dieses Verfah-
ren zu erstatten.

Die auf mich lautenden Vollmachten sind als **Anlagenkonvolut 1** beigelegt.

Inhaltsverzeichnis

A. Vorbemerkung	8
B. Antragsgegenstand	10
C. Zulässigkeit	12
I. Zuständigkeit des Verfassungsgerichtshofs	12
II. Statthafter Antragsgegenstand	13
III. Statthaftigkeit des Antrags	13
IV. Antragsberechtigung	13
V. Objektives Klarstellungsinteresse	13
D. Begründetheit	14
I. §§ 24, 24a, 24e ASOG (Anfertigung und automatisierte Auswertung von Bild- und Tonaufzeichnungen)	14
1. Gesetz und Gesetzesbegründung	14
2. Funktionsweise und Anwendungsszenarien	18
3. Eingriffe in den Schutzbereich	20
a) Erhebung	21
b) Automatisierte Auswertung	22
4. Keine Rechtfertigung	22
a) Eingriffsintensität	24
aa) Aufzeichnung	24
bb) Automatisierte Auswertung	27
(i) Kriterien zur automatisierten Datenanalyse	27
(ii) Übertragung auf die Auswertung von Bild- und Tonaufzeichnungen	30
b) Verletzung der verfassungsrechtlichen Anforderungen	35
aa) Unzureichende Voraussetzungen	35
(i) Veranstaltungen und Ansammlungen	36
(ii) Gefährdete Objekte	36
(iii) Kriminalitätsbelastete Orte	37
bb) Fehlende Festlegung der Verhaltensmuster	40
cc) Fehlende Kenntlichmachung	40
dd) Unzureichende Dokumentationspflicht	41
ee) Fehlende Vorkehrungen gegen Fehler, Diskriminierung und Datenmissbrauch	42

II. §§ 26a, 26b ASOG (Quellen-Telekommunikationsüberwachung und Online-Durchsuchung)	45
1. Gesetz und Gesetzesbegründung	45
2. Funktionsweise und Anwendungsszenarien	48
3. Eingriffe in Schutzbereiche	50
4. Keine Rechtfertigung	53
a) Eingriffsintensität	53
b) Unzureichende Eingriffsvoraussetzungen	54
aa) Rechtsgüterschutz	55
bb) Eingriffsschwelle	61
cc) Unzulässiger dynamischer Verweis	63
c) Fehlende Überprüfung der genutzten Software	64
d) Fehlendes Schwachstellenmanagement	67
aa) Schutzpflicht für die IT-Sicherheit	67
bb) Erfordernis eines Schwachstellenmanagements	70
cc) Fehlen eines Schwachstellenmanagements	72
III. § 28a ASOG (biometrischer Abgleich mit öffentlich zugänglichen Daten)	73
1. Gesetz und Gesetzesbegründung	74
2. Funktionsweise und Anwendungsszenarien	77
3. Verstoß gegen Art. 33 VvB	79
a) Eingriffe in den Schutzbereich	79
b) Keine Rechtfertigung	80
aa) Eingriffsintensität	81
(i) Streubreite	81
(ii) Art der Daten	82
(iii) Verarbeitungsdauer	85
(iv) Folgen des Abgleichs	85
(v) Risiken durch künstliche Intelligenz	85
(vi) Heimlichkeit	86
bb) Verletzung der verfassungsrechtlichen Anforderungen	87
(i) Verstoß gegen das Verbot flächendeckender Überwachung	87
(ii) Kein Ausschluss von sensiblen Daten	89
(iii) Unzureichende Voraussetzungen des Abgleichs	90
(iv) Keine Beschränkung auf Polizeiverantwortliche	91
(v) Kein Schutz vor Diskriminierung	91
4. Verstoß gegen Art. 26 VvB	92
IV. §§ 42a, 42b Abs. 4 Satz 1 ASOG (Zweckbindung und Kennzeichnung)	92

1. Gesetz und Gesetzesbegründung	93
2. Anwendungsszenarien	97
3. Eingriffe in die Schutzbereiche von Grundrechten	97
4. Keine Rechtfertigung	98
V. § 42d ASOG (Training und Testung von KI-Systemen)	100
1. Gesetz und Gesetzesbegründung	100
2. Anwendungsszenarien	103
3. Eingriffe in die Schutzbereiche von Grundrechten	104
4. Keine Rechtfertigung	104
a) Durchbrechung des Grundsatzes der hypothetischen Datenneuerhebung	105
b) Unverhältnismäßigkeit	106
aa) Eingriffsintensität	107
bb) Unzureichende Voraussetzungen	114
cc) Unzureichende Schutzvorkehrungen	115
dd) Befugnis zu Weitergabe	117
VI. § 47a ASOG (automatisierte Datenanalyse)	121
1. Gesetz und Gesetzesbegründung	121
2. Funktionsweise und Anwendungsszenarien	125
3. Eingriffe in den Schutzbereich	126
4. Keine Rechtfertigung	127
a) Analyseplattform	128
aa) Eingriffsintensität	128
bb) Keine ausreichenden Voraussetzungen	131
cc) Fehlende Kennzeichnung	133
b) Datenanalyse	134
aa) Eingriffsintensität	134
(i) Art und Umfang der Daten	134
(ii) Analysemethoden	140
(iii) Heimlichkeit	146
bb) Keine ausreichenden Voraussetzungen	147
(i) Rechtsgüterschutz	148
(ii) Eingriffsschwelle	150
(iii) Unzulässiger dynamischer Verweis	151
(iv) § 47a Abs. 1 Satz 5 ASOG	152
cc) Unzureichende Kennzeichnungspflicht	153
dd) Fehlende Vorkehrungen gegen Fehler, Diskriminierung und Datenmissbrauch	153
ee) Keine ausreichenden Kontrollen	155

A. Vorbemerkung

Der vorliegende Normenkontrollantrag richtet sich gegen Vorschriften des Allgemeinen Gesetz zum Schutz der öffentlichen Sicherheit und Ordnung in Berlin (Allgemeines Sicherheits- und Ordnungsgesetz - ASOG), das durch das Gesetz zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Art. 29 der Verfassung von Berlin vom 11. Dezember 2025 umfassend novelliert wurde.

Mit den Änderungen sollte die Rechtsprechung des Bundesverfassungsgerichts nachgezeichnet werden, was aber nicht durchgehend gelungen ist. Die maßgeblich aus dem Verhältnismäßigkeitsgrundsatz folgenden Anforderungen an die Rechtfertigung schwerer Grundrechtseingriffe wurden nicht eingehalten. Zudem wurden neue, grundrechtlich hochproblematische Instrumente eingeführt.

Datenschutz ist vorgelagerter Grundrechtsschutz. Er soll einerseits ermöglichen, dass die Bürgerinnen und Bürger unbefangen und ohne Angst ihre Grundrechte wahrnehmen. Andererseits soll er verhindern, dass Daten in die falschen Hände geraten. Polizeiliche Befugnisse müssen daher so ausgestaltet sein, dass sie staatliche Macht begrenzen und kontrollierbar machen. Nur so lässt sich sicherstellen, dass sie auch unter geänderten politischen Vorzeichen nicht missbraucht werden, etwa um politische Gegnerinnen und Gegner einzuschüchtern oder Minderheiten zu diskriminieren. Das angegriffene Gesetz wird dem nicht gerecht, sondern ist ein normatives Einfallstor für unverhältnismäßige staatliche Überwachungsmaßnahmen. Im Einzelnen:

- Die §§ 24, 24a und 24e ASOG ermächtigen zur automatisierten Auswertung von im öffentlichen Raum angefertigten Videoaufzeichnungen. Mittels künstlicher Intelligenz soll das Verhalten aller Menschen, die sich in den jeweiligen Bereichen aufhalten, analysiert werden. Das Gesetz sieht dabei weder hinreichend gehaltvolle Voraussetzungen für den Einsatz der Technologie noch ausreichende Schutzvorkehrungen gegen Fehlentscheidungen, Diskriminierung und Datenmissbrauch vor.

- § 26a und § 26b ASOG ermöglichen die Infiltration informationstechnischer Systeme mittels einer speziellen Spähsoftware – dem sogenannten Staatstrojaner. Die Befugnisse setzen einen hochproblematischen Anreiz dafür, dass die Polizei IT-Sicherheitslücken ankauft und offenhält, statt sie umgehend an die Hersteller zu melden. Die Sicherheitslücken können in der Folge auch von Kriminellen oder ausländischen Staaten für Cyberangriffe gegen Privatpersonen, Unternehmen und staatliche Stellen ausgenutzt werden. Das Gesetz gefährdet so die IT-Sicherheit aller Menschen. Der Staat hat jedoch die grundrechtliche Pflicht, die Integrität informationstechnischer Systeme der Bürgerinnen und Bürger zu schützen. Hierfür ist ein Schwachstellenmanagement mit einer klaren Meldepflicht erforderlich.
- § 28a ASOG ermächtigt zum biometrischen Abgleich mit Daten aus dem Internet. Jedes Foto, das unter Umständen 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.
- § 42a i.V.m. § 42b Abs. 4 Satz 1 ASOG lockert die verfassungsrechtlichen Anforderungen an die Zweckbindung polizeilich erhobener Daten. Das Gesetz lässt weitgehende Ausnahmen von der vorgeschriebenen Kennzeichnung personenbezogener Daten zu. Es ist damit nicht sichergestellt, dass einmal erhobene Daten nur unter den verfassungsrechtlich gebotenen Voraussetzungen für andere Zwecke weiterverwendet werden. Insbesondere ist zu befürchten, dass verfassungsrechtlich erforderliche Tatbestandsvoraussetzungen etwa bei der automatisierten Datenanalyse aus Wirtschaftlichkeitserwägungen ignoriert werden.
- § 42d ASOG erlaubt es der Polizei und der Feuerwehr, die bei ihnen gespeicherten personenbezogenen Daten für das Training und die Testung von KI-Systemen zu verwenden. Das Gesetz spezifiziert dabei weder, welche KI-Systeme getestet bzw. trainiert werden

dürfen, noch schränkt es die verwendbaren Daten hinreichend ein. Sehr sensible Daten (z.B. aus einer Telekommunikationsüberwachung) dürfen sogar an private Dritte weitergegeben werden. Das durchbricht den Zweckbindungsgrundsatz und birgt erhebliche Risiken für die betroffenen Personen.

- § 47a ASOG ermöglicht die automatisierte Zusammenführung und Analyse umfangreicher polizeilicher Datenbestände auf einer zentralen Analyseplattform. Es entsteht eine übergreifende und dauerhafte „Super-Datenbank“ aus einer unbestimmten Anzahl an polizeilichen Datenbeständen. Die darin gespeicherten Daten sollen auch mittels künstlicher Intelligenz analysiert werden, ohne dass das Gesetz ausreichende tatbestandliche Voraussetzungen und Vorkehrungen gegen Fehler, Diskriminierung und Datenmissbrauch enthält.

Die Befugnisse verstoßen aus mehreren Gründen gegen Grundrechte. Das angerufene Gericht kann sich dabei weitgehend an der Rechtsprechung des Bundesverfassungsgerichts orientieren, etwa zu den verfassungsrechtlichen Anforderungen an eingriffsintensive Überwachungsmaßnahmen und zweckändernde Datenverarbeitungen, zum Einsatz von Staatstrojanern oder zur automatisierten Datenanalyse. Teilweise müssen jedoch auch neue Maßstäbe entwickelt werden bzw. die bereits entwickelten Maßstäbe auf neuartige Instrumente übertragen werden.

B. Antragsgegenstand

Der Landesgesetzgeber hat am 11. Dezember 2025 das Gesetz zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Art. 29 der Verfassung von Berlin verabschiedet. Dieses ist am 24. Dezember 2025 in Kraft getreten. Durch die Reform wurden die Befugnisse zur Datenerhebung und -weiterverarbeitung ausgeweitet,

GVBl. Nr. 36/2025, S. 590.

Insbesondere wurden die Befugnisse zur Datenerhebung durch den Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufzeichnungen (sogenannte Videoüberwachung) ausgeweitet und

um eine Befugnis zur automatisierten Auswertung (sogenannte intelligente Videoüberwachung) ergänzt (§§ 24, 24a, 24e ASOG).

Die schon bestehende Befugnis zur Telekommunikationsüberwachung (§ 26 ASOG) wurde um Befugnisse zur Telekommunikationsüberwachung informationstechnischer Systeme (§ 26a ASOG, sogenannte Quellen-Telekommunikationsüberwachung) und zum verdeckten Eingriff in informationstechnische Systeme (§ 26b ASOG, sogenannte Online-Durchsuchung) ergänzt.

Zudem wurde eine Befugnis für den nachträglichen biometrischer Abgleich mit öffentlich zugänglichen Daten aus dem Internet geschaffen (§ 28a ASOG).

Der neue § 42b ASOG enthält eine Pflicht zur Kennzeichnung von personenbezogenen Daten, die in Informationssystemen gespeichert sind. Dies dient der Einhaltung des Zweckbindungsgrundsatzes. Nach § 42b Abs. 4 Satz 1 gilt die Kennzeichnungspflicht jedoch nicht, soweit die Kennzeichnung tatsächlich nicht möglich ist, technisch nicht möglich ist oder einen unverhältnismäßigen technischen Aufwand erfordern würde. Erst ab dem 1. Januar 2031 kann nur noch bei tatsächlicher Unmöglichkeit auf die Kennzeichnung verzichtet werden.

Neu sind zudem die Befugnis zur Verarbeitung personenbezogener Daten für das Training und die Testung von KI-Systemen (§ 42d ASOG) und zur automatisierten Datenanalyse (§ 47a ASOG).

Das Änderungsgesetz geht auf einen Antrag der Fraktion der CDU und der Fraktion der SPD zurück,

Abgh-Drs. 19/2553; der parlamentarische Vorgang ist abrufbar unter <https://pardok.parlament-berlin.de/portala/vorgang/V-435192>.

Zur Anhörung im Ausschuss für Inneres, Sicherheit und Ordnung am 29. September 2025 haben die Sachverständigen schriftliche Stellungnahmen abgegeben,

Berliner Beauftragte für Datenschutz und Informationsfreiheit, Stellungnahme zum Gesetzentwurf zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 2**; Botta, Stellungnahme zum

Gesetz zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 3**; Möstl, Schriftliche Stellungnahme im Rahmen der Anhörung des Abgeordnetenhauses Berlin zum Entwurf eines Gesetzes zur Reform des Berliner Polizei- und Ordnungsrechts (Drs. 19/2553), **Anlage 4**; Gesellschaft für Freiheitsrechte e.V., 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), **Anlage 5**.

In der Sitzung vom 17. November 2025 stellten die Fraktion der CDU und die Fraktion der SPD einen Änderungsantrag,

Änderungsantrag der Fraktion der CDU und der Fraktion der SPD zur Drucksache 19/2553, **Anlage 6**.

Hierzu gab die Berliner Beauftragte für Datenschutz und Informationsfreiheit eine weitere Stellungnahme ab,

Berliner Beauftragte für Datenschutz und Informationsfreiheit, Stellungnahme zum Änderungsantrag der Fraktion der CDU und der Fraktion der SPD zur Drucksache 19/2553: Gesetz zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 7**.

Die angegriffenen Normen werden unten im Zusammenhang mit der Begründetheit ausführlich dargestellt.

C. Zulässigkeit

Der abstrakte Normenkontrollantrag ist zulässig.

I. Zuständigkeit des Verfassungsgerichtshofs

Die Zuständigkeit des Verfassungsgerichtshofs des Landes Berlin ergibt sich aus Art. 84 Abs. 7 Nr. 2 VvB i.V.m § 14 Nr. 4 VerfGHG.

Danach entscheidet der Verfassungsgerichtshof bei Meinungsverschiedenheiten oder Zweifeln über die förmliche oder sachliche Vereinbarkeit von Landesrecht mit der Verfassung von Berlin auf Antrag des Senats oder eines Viertels der Mitglieder des Abgeordnetenhauses. Die Antragstellenden halten die angegriffenen Normen für mit der Verfassung von Berlin unvereinbar.

II. Statthafter Antragsgegenstand

Art. 84 Abs. 7 Nr. 2 VvB, §§ 14 Nr. 4, 43 VerfGHG setzen Landesrecht als Antragsgegenstand voraus.

Bei den mit dem Normenkontrollantrag angegriffenen Vorschriften des ASOG handelt es sich um ein in Kraft getretenes Parlamentsgesetz des Landes Berlin und damit um einen tauglichen Antragsgegenstand im Sinne des Art. 84 Abs. 7 Nr. 2 VvB, § 14 Nr. 4, § 43 VerfGHG.

III. Statthaftigkeit des Antrags

Der Antrag ist statthaft. Art. 84 Abs. 7 Nr. 2 VvB setzt Zweifel über die förmliche oder sachliche Vereinbarkeit von Landesrecht mit der Verfassung von Berlin voraus. Nach § 43 Nr. 1 VerfGHG müssen die Antragsberechtigten das Landesrecht wegen seiner förmlichen oder sachlichen Unvereinbarkeit mit der Verfassung von Berlin für nichtig halten. Die Antragstellenden halten die mit dem Normenkontrollantrag angegriffenen Vorschriften wegen ihrer sachlichen Unvereinbarkeit mit der Verfassung von Berlin für nichtig.

IV. Antragsberechtigung

Die Antragstellenden sind antragsberechtigt. Nach Art. 84 Abs. 7 Nr. 2 und § 43 VerfGHG sind ein Viertel der Mitglieder des Abgeordnetenhauses antragsberechtigt. Vorliegend wird der Antrag von 53 Abgeordneten, nämlich den Abgeordneten der Fraktionen Bündnis 90/Die Grünen und Die Linke, gestellt. Dem Abgeordnetenhaus gehören derzeit 159 Abgeordnete an. Demnach handelt es sich bei den 53 Abgeordneten um ca. 33 Prozent, also mehr als ein Viertel der Mitglieder des Abgeordnetenhauses.

V. Objektives Klarstellungsinteresse

Die Antragstellenden haben ein objektives Klarstellungsinteresse.

Das objektive Klarstellungsinteresse wird durch die von den Antragstellern dargelegten Zweifel an der Gültigkeit der Normen indiziert,

VerfGH Berlin, Beschluss vom 18. Juni 2014 – 165/12 –, Rn. 27.

Ein darüber hinaus gehendes Rechtsschutzinteresse ist nicht erforderlich,

BVerfG, Urteil vom 24. Juli 1979 – 2 BvF 1/78 –, Rn. 60.

D. Begründetheit

Der Antrag ist begründet. Die angegriffenen Normen sind mit der Verfassung von Berlin unvereinbar.

I. §§ 24, 24a, 24e ASOG (Anfertigung und automatisierte Auswertung von Bild- und Tonaufzeichnungen)

Die §§ 24, 24a, 24e ASOG verstoßen gegen das Recht auf informationelle Selbstbestimmung nach Art. 33 VvB.

Die Normen (1.) ermächtigen nicht nur zur Erstellung von Bild- und Tonaufzeichnungen, sondern auch zur automatisierten Auswertung dieser Daten (2.). Beide Maßnahmen stellen eigenständige Grundrechtseingriffe dar (3.). Diese Eingriffe sind nicht gerechtfertigt (4.). Sie greifen erheblich in das Grundrecht auf informationelle Selbstbestimmung ein (4. a)), ohne dass im Gesetz hinreichende Eingriffsvoraussetzungen vorgesehen sind (4. b) aa)). Die automatisierte Auswertung ist zudem unverhältnismäßig, weil die zu erkennenden Verhaltensmuster nicht festgelegt sind (4. b) bb)). Ferner fehlt es teilweise an einer Kenntlichmachung der Überwachung (4. b) cc)), einer Dokumentationspflicht (4. b) dd)) sowie ausreichende Schutzvorkehrungen gegen Fehlentscheidungen, Diskriminierung und Datenmissbrauch (4. b) ee)).

1. Gesetz und Gesetzesbegründung

Die §§ 24, 24a, 24e ASOG ermächtigen die Polizei zur Datenerhebung durch Anfertigung von Bildaufzeichnungen bei öffentlichen Veranstaltungen oder Ansammlungen (§ 24 AOSG), an und in gefährdeten Objekten (§ 24a ASOG) und an kriminalitätsbelasteten Orten (§ 24e ASOG). § 24 ASOG ermöglicht auch Tonaufzeichnungen.

Die Polizei kann alle Daten nach §§ 24 Abs. 1 Satz 4, 24a Abs. 1 Satz 2 und 24e Abs. 4 ASOG automatisiert auswerten.

Die Normen haben folgenden Wortlaut:

§ 24

Datenerhebung bei öffentlichen Veranstaltungen und Ansammlungen

(1) Die Polizei kann bei oder im Zusammenhang mit öffentlichen, nicht dem Versammlungsfreiheitsgesetz Berlin unterliegenden Veranstaltungen oder Ansammlungen personenbezogene Daten durch Ermittlungen oder durch den Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufzeichnungen von Teilnehmern erheben, wenn Tatsachen die Annahme rechtfertigen, dass dabei Straftaten begangen werden. Dabei dürfen auch personenbezogene Daten über Dritte erhoben werden, soweit das unvermeidbar ist, um eine Datenerhebung durchführen zu können. Verdeckte Bild- und Tonaufzeichnungen sind unzulässig. Die Polizei kann die angefertigten Bildaufnahmen und -aufzeichnungen auch automatisiert auswerten; § 24e Absatz 4 gilt entsprechend.

(2) Bild- und Tonaufzeichnungen, daraus sowie bei Ermittlungen nach Absatz 1 gewonnene personenbezogene Daten sind spätestens zwei Monate nach der Datenerhebung zu löschen oder zu vernichten, soweit diese nicht zur Verfolgung von Straftaten oder Ordnungswidrigkeiten benötigt werden oder Tatsachen die Annahme rechtfertigen, dass die Person künftig Straftaten von erheblicher Bedeutung begehen wird. Die §§ 42c, 42d und 48 Absatz 6 bleiben unberührt, ebenso § 44 Absatz 3 des Berliner Datenschutzgesetzes.

(3) Bei oder im Zusammenhang mit öffentlichen, nicht dem Versammlungsfreiheitsgesetz Berlin unterliegenden Großveranstaltungen, die im Rahmen einer vom übrigen Straßenland sichtbar unterschiedenen Sondernutzung durchgeführt werden, dürfen Polizei und Rettungsdienste zur Erfüllung ihrer jeweiligen Aufgaben die Bildaufnahmen verarbeiten, die von der Veranstalterin oder dem Veranstalter gemäß § 20 des Berliner Datenschutzgesetzes oder § 4 des Bundesdatenschutzgesetzes zur ordnungsgemäßen Durchführung der Veranstaltung gefertigt werden. Großveranstaltungen sind Veranstaltungen, die nach Art und Größe die Annahme rechtfertigen, dass erhebliche Gefahren für die öffentliche Sicherheit entstehen können.

(4) § 24f bleibt unberührt.

§ 24a

Datenerhebung an und in gefährdeten Objekten

(1) Zur Erfüllung ihrer Aufgaben nach § 1 Absatz 3 kann die Polizei an oder in einem gefährdeten Objekt, insbesondere einem Gebäude, auch einem Amts- oder Dienstgebäude, oder einem sonstigen Bauwerk von öffentlichem Interesse, einer Religionsstätte, einem Denkmal oder einem Friedhof, einschließlich der jeweils zugehörigen Parkplätze und sonstigen Außenflächen, oder, soweit zur Zweckerreichung zwingend erforderlich, den unmittelbar im Zusammenhang mit dem Objekt stehenden Grün- oder Straßenflächen personenbezogene Daten durch Anfertigung von Bildaufnahmen erheben und die Bilder zur Beobachtung übertragen und aufzeichnen, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass an oder in einem Objekt dieser Art Straftaten drohen. Die Polizei kann die angefertigten Bildaufnahmen und -aufzeichnungen auch automatisiert auswerten; § 24e Absatz 4 gilt entsprechend.

(2) Der Umstand der Beobachtung und Aufzeichnung und die datenverarbeitende Stelle sind durch Beschilderung kenntlich zu machen.

(3) Bildaufnahmen und -aufzeichnungen sind spätestens nach einem Monat zu vernichten oder zu löschen, soweit sie nicht zur Verfolgung von Straftaten benötigt werden oder Tatsachen die Annahme rechtfertigen, dass die Person künftig Straftaten von erheblicher Bedeutung begehen wird. § 24 Absatz 2 Satz 2 gilt entsprechend.

(4) Werden durch eine Maßnahme nach Absatz 1 erhobene Daten einer bestimmten Person zugeordnet, so ist diese nach § 42 des Berliner Datenschutzgesetzes über eine Verarbeitung zu benachrichtigen, soweit die Daten nicht nach Absatz 3 zu einem der dort genannten Zwecke benötigt oder gelöscht oder vernichtet werden. § 27d Absatz 3 Satz 3 bis 5 gilt entsprechend.

§ 24e

Datenerhebung an kriminalitätsbelasteten Orten

(1) Zur Erfüllung ihrer Aufgaben nach § 1 Absatz 3 kann die Polizei an kriminalitätsbelasteten Orten personenbezogene Daten durch Anfertigung von Bildaufnahmen erheben und die Bilder zur Beobachtung übertragen und aufzeichnen. Die Maßnahme erfolgt auf Anordnung der Polizeipräsidentin oder des Polizeipräsidenten oder der Vertretung im Amt. Die Auswirkungen einer solchen Maßnahme auf die Kriminalität an dem jeweiligen Ort sind mindestens alle zwei Jahre zu untersuchen; anschließend ist über die Maßnahme unverzüglich erneut zu entscheiden. Über die Ergebnisse unterrichtet der Senat das Abgeordnetenhaus.

(2) Die Anordnung der Datenerhebung ist zu dokumentieren. Der Umstand der Beobachtung und Aufzeichnung sowie die datenverarbeitende Stelle sind zudem durch Beschilderung kenntlich zu machen. Die Polizei Berlin gibt öffentlich bekannt, an welchen Orten Datenerhebungen nach dieser Vorschrift erfolgen.

(3) § 24a Absatz 3 und 4 gilt entsprechend.

(4) Die Polizei kann die nach Absatz 1 angefertigten Bildaufnahmen und -aufzeichnungen auch automatisiert auswerten. Die automatisierte Auswertung darf nur auf das Erkennen solcher Verhaltensmuster ausgerichtet sein, die auf die Begehung einer Straftat oder den Eintritt eines Unglücksfalls im Sinne von § 323c Absatz 1 des Strafgesetzbuches hindeuten. Ein automatisiertes Auslösen behördlicher Maßnahmen auf Grund einer automatisierten Auswertung, die automatisierte biometrische Fernidentifizierung sowie die Nutzung der Bildaufnahmen und -aufzeichnungen für das Testen oder Trainieren von Programmen zur biometrischen Fernidentifizierung sind ausgeschlossen. Erst nach Sichtung der betreffenden Bildaufnahmen und -aufzeichnungen oder der Inaugenscheinnahme der Lage vor Ort dürfen weitere Maßnahmen ergriffen werden, die sich gegen bestimmte Personen richten. Absatz 1 Satz 2 sowie Absatz 2 Satz 1 gelten entsprechend.

Die in § 24e Abs. 1 Satz 1 ASOG genannten kriminalitätsbelasteten Orte werden nach § 17a ASOG grundsätzlich per Rechtsverordnung festgelegt. Die Norm hat folgenden Wortlaut:

§ 17a

Kriminalitätsbelastete Orte; Verordnungsermächtigung

(1) Die für Inneres zuständige Senatsverwaltung wird ermächtigt, durch Rechtsverordnung bestimmte Straßen, Wege, Plätze oder sonstige Bereiche als kriminalitätsbelastete Orte einzustufen. Dies ist nur für solche Orte zulässig, die öffentlich zugänglich sind und von denen Tatsachen die Annahme rechtfertigen, dass dort Personen Straftaten von erheblicher Bedeutung verabreden, vorbereiten oder verüben.

(2) Die Polizeipräsidentin oder der Polizeipräsident oder die Vertretung im Amt kann die Einstufung eines Bereichs als kriminalitätsbelasteter Ort unter den Voraussetzungen des Absatzes 1 für die Dauer von insgesamt höchstens einem Monat im jeweiligen Kalenderjahr durch Allgemeinverfügung vornehmen, wenn Maßnahmen nach diesem Gesetz, die diese Einstufung voraussetzen, keinen Aufschub dulden und der Erlass einer Rechtsverordnung voraussichtlich nicht rechtzeitig erfolgen würde. In besonderen Eilfällen kann die öffentliche Bekanntgabe der Allgemeinverfügung dadurch erfolgen, dass ihr verfügender Teil auf der Internetseite der Polizei Berlin zugänglich gemacht und zusätzlich durch weitere geeignete Nachrichtennittel verbreitet wird. Dabei kann bestimmt werden, dass die Allgemeinverfügung mit der Zugänglichmachung auf einer Internetseite der Polizei Berlin als bekanntgegeben gilt. Über den Erlass jeder Allgemeinverfügung unterrichtet die für Inneres zuständige Senatsverwaltung unverzüglich das Abgeordnetenhaus.

(3) Die für Inneres zuständige Senatsverwaltung unterrichtet das Abgeordnetenhaus über die Gründe, die zur Einstufung als kriminalitätsbelasteter Ort geführt haben. Der Senat unterrichtet das Abgeordnetenhaus zudem jährlich über die an den kriminalitätsbelasteten Orten nach diesem Gesetz getroffenen Maßnahmen.

Das ASOG ermöglicht schon länger die Datenerhebung bei öffentlichen Veranstaltungen und Ansammlungen sowie an gefährdeten Objekten. Durch das Gesetz vom 11. Dezember 2025 wurde letztgenannte Befugnis auf die Datenverarbeitung **in** gefährdeten Objekten ausgeweitet. Zudem wurde eine neue Befugnis zur Datenerhebung an kriminalitätsbelasteten Orten geschaffen,

Gesetz zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Art. 29 der Verfassung von Berlin vom 11. Dezember 2025, GVBl. Nr. 36/2025, S. 590, 594 f; Abgh-Drs. 19/2553, S. 158.

Die Datenerhebungsbefugnisse wurden zudem durch Befugnisse zur automatisierten Auswertung ergänzt. Laut der Gesetzesbegründung ist das Ziel, tätliche Auseinandersetzungen, Unglücksfälle oder andere besondere Situationen rechtzeitig zu erkennen. Dabei gebe die Technik den Polizeidienstkräften lediglich ein Signal, sich die betreffende Videoübertragung genauer anzusehen; die Datenanalyse geschehe somit nur zu dem Zweck, die Aufmerksamkeit der eingesetzten Kräfte zu unterstützen. Es handele sich um ein Assistenzsystem,

Abgh-Drs. 19/2553, S. 118 und 166.

Eine automatisierte biometrische Fernidentifizierung sei ausgeschlossen, wobei der Begriff sich an dem der „biometrischen Fernidentifizierung“ im Sinne des Art. 3 Nr. 41 der Verordnung (EU) 2024/1689 (KI-Verordnung) orientiere,

Abgh-Drs. 19/2553, S. 118 und 166 f.

Unklar ist, was unter der „automatisierten“ biometrischen Fernidentifizierung, die nach § 24e Abs. 4 Satz 3 ASOG ausgeschlossen ist, zu verstehen ist. Die Formulierung lässt Raum für eine „manuelle“ biometrische Fernidentifizierung.

2. Funktionsweise und Anwendungsszenarien

Die Befugnis ist technikoffen gestaltet, sodass insbesondere bei der Funktionsweise der automatisierten Auswertung große Gestaltungsmöglichkeiten bestehen.

Systeme zur Verhaltensmustererkennung gibt es bereits in Mannheim und Hamburg. Dabei kommt jeweils eine Software vom Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung (IOSB) zum Einsatz, die mittels einer „digitalen Skelettierung“ atypische Bewegungsmuster erkennen soll,

hierzu Arzt, in: Lisken/Denninger/Bäcker PolR-HdB, 8. Aufl. 2026, Kap. 6 Rn. 1419.

Die Verhaltenserkennung ist nach derzeitigem Stand der Technik fehleranfällig. Es kommt zu einer erheblichen Anzahl an Falsch-Positiv-Meldungen, also Fällen, in denen ein Hinweis gegeben wird, obwohl kein polizeilich relevantes Verhalten vorliegt (weil zum Beispiel eine Umarmung als körperliche Auseinandersetzung erkannt wird),

Weizenbaum-Institut, Stellungnahme zur Novellierung des Allgemeinen Sicherheits- und Ordnungsgesetzes Berlin (ASOG Bln), Policy Paper #19, März 2026, S. 15 f. m.w.N.

Welche Verhaltensmuster erkannt werden sollen, schreibt § 24e Abs. 4 ASOG nicht vor. Nach der Ausschreibung zu einem Pilotprojekt an gefährdeten Objekten soll die Software verschiedene Szenarien

erkennen. Dazu zählt beispielsweise das Betreten gesperrter Bereiche oder das Beschädigen von Zäunen, aber auch „Langes Verharren/Umhergehen ohne Anlass“ und „Wiederholtes Erscheinen (ohne biometrische Identifikation)“,

Polizei Berlin, Leistungsverzeichnis Projekt zur Erprobung KI-gestützter Videotechnik im Objektschutz der Polizei Berlin, **Anlage 8**, S. 7.

Wie das wiederholte Erscheinen ohne biometrische Identifikation erkannt werden soll, bleibt offen. Das Erkennungsziel zeigt jedoch, dass Personen auch über einen längeren Zeitraum, unter Umständen auch über mehrere Kameras und Orte hinweg überwacht werden können.

Die Leistungsbeschreibung zum Pilotprojekt „Videoschutz an kriminalitätsbelasteten Orten“ nennt als zwingend zu erkennende Szenarien „Körperliche Auseinandersetzungen (z.B. Schlagen, Treten, Kämpfen)“ und „Stürzende / liegende Personen“. Als zusätzliche optionale Erkennungsszenarien werden im Anforderungskatalog unter anderem die „Erkennung herrenloser Gegenstände“ und die Erkennung von „Wurfbewegungen“ genannt,

Polizei Berlin, Leistungsbeschreibung Videoschutz an kriminalitätsbelasteten Orten, **Anlage 9**, S. 14 f.; Anlage A.2.1 – Anforderungenkatalog, **Anlage 10**, S. 10 f.

Auch diese Szenarien deuten in vielen Fällen nicht auf Straftaten oder Unglücksfälle hin; etwa wenn ein Gegenstand vergessen oder ein Ball für einen Hund geworfen wird. Jedenfalls sind die Szenarien hochgradig interpretationsbedürftig und dürften zu einer hohen Zahl an Fehlmeldungen führen.

Als Muss-Anforderung wird definiert: „Das KI-System für die Kernszenarien körperliche Auseinandersetzung und stürzende/liegende Person nachweisbare Leistungskennzahlen von $\geq 85\%$ Precision, $\geq 80\%$ Recall und $\leq 5\%$ False Positive Rate gewährleisten“,

Anlage A.2.1 – Anforderungenkatalog, **Anlage 10**, S. 10.

Eine Falsch-Positiv-Rate von 5 % erscheint auf den ersten Blick gering. Bei einer kontinuierlichen Überwachung mit Millionen unauffälliger

Bewegungen führt dies aber dennoch zu einer sehr hohen absoluten Zahl von Fehlalarmen.

Den Zuschlag für das Pilotprojekt an kriminalitätsbelasteten Orten hat inzwischen die Adesso SE erhalten, ein Unternehmen, das bereits von einem schwerwiegenden Sicherheitsvorfall betroffen war,

netzpolitik.org vom 14. Juli 2026, Adesso SE baut Verhaltensscanner für die Polizei, <https://netzpolitik.org/2026/videoueberwachung-in-berlin-adesso-se-baut-verhaltensscanner-fuer-die-polizei/>.

Erste Kameras sollen am kriminalitätsbelasteten Ort Kottbusser Tor installiert werden,

rbb24.de vom 4. August 2026, Polizei startet Pilotprojekt zur Videoüberwachung am Kottbusser Tor, <https://www.rbb24.de/politik/beitrag/2026/08/videokameras-ki-kottbusser-tor-berlin-polizei-ueberwachung.html>.

3. Eingriffe in den Schutzbereich

Die Erstellung von Bild- und Tonaufzeichnungen und ihre Auswertung greifen in das Recht des einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen, aus Art. 33 VvB ein.

Art. 33 VvB gewährleistet das aus dem Gedanken der Selbstbestimmung folgende Recht des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden. Das Grundrecht gewährt seinen Trägern Schutz gegen unbegrenzte Erhebung, Speicherung, Verwendung oder Weitergabe der auf sie bezogenen, individualisierten oder individualisierbaren Daten,

vgl. VerfGH Berlin, Beschluss vom 14. Februar 2006 – 34/03 –, Rn. 27.

Das in Art. 33 VvB bzw. zuvor in Art. 21b VvB 1950 geschützte Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen, entspricht dem aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG hergeleiteten Recht auf informationelle Selbstbestimmung. Da beide Grundrechte

deckungsgleich sind, ist die Rechtsprechung des Bundesverfassungsgerichts zum Grundrecht auf informationelle Selbstbestimmung uneingeschränkt auf Art. 33 VvB übertragbar,

vgl. VerfGH Berlin, Beschluss vom 14. Mai 2014 – 151/11 –, Rn. 119, 123; Beschluss vom 17. Dezember 1997 – 2/96 –, Rn. 11; Siegel, in: BeckOK Verfassung Berlin BlnVerf, 5. Edition, Stand: 01.05.2026, Art. 33 Rn. 3.

Bei Verarbeitung personenbezogener Daten ist vorrangig Art. 33 VvB als Spezialvorschrift zu Art. 6 und 7 VvB heranzuziehen,

vgl. Siegel, in: BeckOK Verfassung Berlin BlnVerf, 5. Edition, Stand: 01.05.2026, Art. 33 Rn. 1; VerfGH Berlin, Beschluss vom 13. Dezember 2005 – 113/05 –, Rn. 21.

Vorschriften, die zum Umgang mit personenbezogenen Daten durch staatliche Behörden ermächtigen, begründen in der Regel verschiedene, aufeinander aufbauende Eingriffe. Insbesondere ist insoweit zwischen der Erhebung, Speicherung und Verwendung von Daten zu unterscheiden,

VerfGH Berlin, Beschluss vom 14. Mai 2014 – 151/11 –, Rn. 123.

Vorliegend begründen die Erhebung der Daten (a)) und die anschließende automatisierte Auswertung (b)) eigenständige Eingriffe.

a) Erhebung

Bereits die Aufzeichnung als solche greift in das Recht auf informationelle Selbstbestimmung nach Art. 33 VvB ein,

vgl. BVerfG, Beschluss vom 23. Februar 2007 – 1 BvR 2368/06 –, Rn. 37.

Videoüberwachung beeinträchtigt alle, die die betroffenen Orte besuchen, und dient dazu, belastende hoheitliche Maßnahmen vorzubereiten und das Verhalten der den Raum nutzenden Personen zu lenken.

Lediglich eine Videobeobachtung mit bloßer Übersichtsperspektive ohne Aufzeichnung gemäß § 1 Abs. 3 VersammlG Bln a.F. bzw. § 18 Abs. 2 VersFG BE greift nicht in das gemäß Art. 33 VvB gewährleistete Recht ein, soweit eine Identifizierung einzelner Personen unmöglich

oder verboten ist. In diesem Fall werden keine personenbezogenen Daten verarbeitet,

vgl. VerfGH Berlin, Urteil vom 11. April 2014 – 129/13 –, Rn. 50.

Die §§ 24, 24a und 24e ASOG ermächtigen hingegen nicht lediglich zu Übersichtsaufnahmen.

Der Eingriff in das Grundrecht entfällt nicht dadurch, dass lediglich Verhaltensweisen im öffentlichen Raum erhoben werden. Das allgemeine Persönlichkeitsrecht gewährleistet nicht allein den Schutz der Privat- und Intimsphäre, sondern trägt in Gestalt des Rechts auf informationelle Selbstbestimmung auch den informationellen Schutzinteressen des Einzelnen, der sich in die Öffentlichkeit begibt, Rechnung,

vgl. BVerfGE 65, 1 <45>; BVerfG, Beschluss vom 23. Februar 2007 – 1 BvR 2368/06 –, Rn. 39.

Von einer den Eingriff ausschließenden Einwilligung in die Informationserhebung kann selbst dann nicht generell ausgegangen werden, wenn die Betroffenen aufgrund einer entsprechenden Beschilderung wissen, dass sie gefilmt werden. Das Unterlassen eines ausdrücklichen Protests kann nicht mit einer Einverständniserklärung gleichgesetzt werden,

vgl. BVerfG, Beschluss vom 23. Februar 2007 – 1 BvR 2368/06 –, Rn. 40.

b) Automatisierte Auswertung

Die automatisierte Auswertung der Videoüberwachung nach § 24 Abs. 1 Satz 4, § 24a Abs. 1 Satz 2, § 24e Abs. 4 ASOG stellt einen eigenständigen Eingriff in den Schutzbereich des Rechts auf informationelle Selbstbestimmung nach Art. 33 VvB dar,

vgl. BVerfGE 150, 244 <265 f. Rn. 42 ff.>; Bäcker, Kriminalpräventionsrecht, 2015, S. 421.

4. Keine Rechtfertigung

Die Grundrechtseingriffe sind nicht gerechtfertigt.

Das Recht auf informationelle Selbstbestimmung kann nach Art. 33 Satz 2 und 3 VvB zum Schutz überwiegender Allgemeininteressen durch Gesetz beschränkt werden. Dabei muss jeder Eingriff dem Verhältnismäßigkeitsgrundsatz genügen, also ein legitimer Zweck verfolgt werden, und das gewählte Mittel muss zur Erreichung dieses Zwecks geeignet, erforderlich und angemessen sein.

Während die Bildübertragung vor allem dazu dient, der Polizei ein schnelles Einschreiten zu ermöglichen, hat die Aufzeichnung eine Dokumentationsfunktion: Die Dokumentation soll vor allem spätere Strafverfolgung ermöglichen und damit eine abschreckende Wirkung entfalten,

vgl. Bäcker, Kriminalpräventionsrecht, 2015, S. 412 ff.

Wissenschaftliche Untersuchungen, lassen jedoch an der Geeignetheit zweifeln. Es gibt kaum empirische Nachweise zur Wirksamkeit von Videoüberwachung. Zudem besteht die Gefahr von Verlagerungseffekten,

vgl. Röhl/Brink, LKRZ 2011, 330; Bäcker, Kriminalpräventionsrecht, 2015, S. 415 f.; Glaubitz u.a., Ergebnisse der Evaluation der polizeilichen Videobeobachtung in Nordrhein-Westfalen gemäß § 15a PolG NRW, Kriminologisches Forschungsinstitut Niedersachsen e.V. Forschungsbericht Nr. 143, 2018, S. 36 ff., Kowalik, Die hoheitliche Videoüberwachung des öffentlichen Raums zur Kriminalprävention. Rechtsgrundlagen, praktische Anwendungsbereiche und präventive Wirksamkeit, 2021, jeweils m.w.N.

Die automatisierte Auswertung soll als „Assistenzsystem“ die Interventionsfunktion stärken und kann auch auf die Dokumentationsfunktion einwirken, wenn das Erkennen einer Straftat dazu führt, dass die Videoaufnahmen für Folgemaßnahmen genutzt werden. Im Kern dient die automatisierte Auswertung jedoch dem Zweck, eine menschliche Sichtung (teilweise) zu ersetzen. Das wirft Fragen nach der Erforderlichkeit auf. Ob die automatisierte Auswertung tatsächlich effizienter ist als die menschliche Sichtung, ist mit Blick auf die hohen Kosten und die Fehleranfälligkeit zweifelhaft,

vgl. Abgeordnetenhaus, Hauptausschuss-Drs. 2875, abrufbar unter <https://www.parlament-berlin.de/adosservice/19/Hauptvorgang/h19->

[2875-v.pdf](#); danach belaufen sich die Kosten für das Pilotprojekt zur Videoüberwachung an kriminalitätsbelasteten Orten in den Jahren 2026 bis 2027 auf 2,47 Mio. € an Investitionskosten und 2,13 Mio. € an Betriebskosten. Das Pilotprojekt für die Videoüberwachung an ausgewählten gefährdeten Objekten soll 1,76 Mio. € an Investitionskosten und 355.000 € an Betriebskosten verursachen. Außerdem entstehe ein Mehrbedarf von neun Dienstkräften (IT-Spezialisten).

Ob die angegriffenen Normen sich noch als geeignet und erforderlich erweisen, kann dahinstehen. Jedenfalls sind sie nicht verhältnismäßig im engeren Sinne. Die Zweifel an der Geeignetheit und Erforderlichkeit müssen in diesem Rahmen berücksichtigt werden.

Wie streng die Anforderungen, die sich aus der Verhältnismäßigkeit im engeren Sinne ergeben, im Einzelnen sind, bestimmt sich in erster Linie nach dem Eingriffsgewicht der Maßnahme (a)). Die angegriffenen Vorschriften genügen diesen Anforderungen nicht (b)).

a) Eingriffsintensität

Bei der Bestimmung der Eingriffsintensität ist zwischen der Aufzeichnung (aa)) und der automatisierten Auswertung (bb)) zu unterscheiden.

aa) Aufzeichnung

Maßgebend für die rechtliche Beurteilung der Intensität eines Eingriffs in das Recht auf informationelle Selbstbestimmung ist die Art der Beeinträchtigung.

Die Videoaufzeichnung betrifft eine Vielzahl von Personen, die sich in den betroffenen Bereichen aufhalten und bewegen. Dass es sich um sehr stark frequentierte Bereiche handeln kann, zeigen beispielsweise die kriminalitätsbelasteten Orte Kottbusser Tor und Warschauer Brücke, die auch als Verkehrsachsen dienen.

Auch von Belang ist, ob die betroffenen Personen für die Maßnahme einen Anlass geben und wie dieser beschaffen ist. Eingriffe mit großer Streubreite, bei denen zahlreiche Personen in den Wirkungsbereich einer Maßnahme einbezogen werden, die in keiner Beziehung zu einem konkreten Fehlverhalten stehen und den Eingriff durch ihr Verhalten

nicht veranlasst haben, weisen grundsätzlich eine hohe Eingriffsintensität auf,

BVerfG, Beschluss der 1. Kammer des Ersten Senats vom 23. Februar 2007 – 1 BvR 2368/06 –, Rn. 51; vgl. Verfassungsgerichtshof des Landes Berlin, Beschluss vom 28. Mai 2004 – 81/02 –, Rn. 26.

Die Videoüberwachung ist daher ein intensiver Eingriff. Sie beeinträchtigt alle, die den betroffenen Raum betreten. Sie dient dazu, belastende hoheitliche Maßnahmen vorzubereiten und das Verhalten der den Raum nutzenden Personen zu lenken. Von den erfassten Personen dürfte nur eine Minderheit gegen Rechtsvorschriften verstoßen. Die Videoüberwachung erfasst daher – wie bei solchen Maßnahmen stets – überwiegend Personen, die selbst keinen Anlass schaffen, dessentwegen die Überwachung vorgenommen wird,

vgl. BVerfG, Beschluss der 1. Kammer des Ersten Senats vom 23. Februar 2007 – 1 BvR 2368/06 –, Rn. 52.

Eingriffsintensivierend kommt hinzu, dass die Bildaufnahmen – anders als bei einer bloßen Videobeobachtung – aufgezeichnet und gespeichert werden,

Bäcker, Kriminalpräventionsrecht, 2015, S. 424.

Das durch die Aufzeichnung gewonnene Bildmaterial kann in vielfältiger Weise ausgewertet, bearbeitet und mit anderen Informationen verknüpft werden,

vgl. BVerfG, Beschluss der 1. Kammer des Ersten Senats vom 23. Februar 2007 – 1 BvR 2368/06 –, Rn. 52.

Die Löschfrist nach § 24 Abs. 2 Satz 1 ASOG beträgt zwei Monate, nach § 24a Abs. 3 Satz 1 und § 24e Abs. 3 ASOG einen Monat. In bestimmten Fällen können die Aufzeichnungen nach diesen Vorschriften sogar länger gespeichert werden,

kritisch dazu die Berliner Beauftragte für Datenschutz und Informationsfreiheit, Stellungnahme zum Gesetzentwurf zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 2**, S. 2 f.

Eingriffsmildernd wirkt sich aus, dass die Daten offen erhoben werden,

vgl. BVerfGE 150, 244 <283 Rn. 97>.

Eine Hinweis- oder Kennzeichnungspflicht gibt es jedoch bei der Datenerhebung bei öffentlichen Veranstaltungen und Ansammlungen nach § 24 ASOG nicht,

näher dazu unten cc).

Eingriffsmildernd wirkt sich zudem aus, dass die Daten grundsätzlich im öffentlichen Raum erhoben werden,

vgl. BVerfGE 150, 244 <283 Rn. 97>.

Dies gilt jedoch im Falle des § 24a ASOG nicht in jedem Fall. Die Norm wurde auf Innenräume ausgeweitet. Sie verlangt aber keine öffentliche Zugänglichkeit dieser Räume. Daher kann die Datenerhebung auch in geschlossenen Räumlichkeiten erfolgen, die nicht frei zugänglich sind,

kritisch dazu die Berliner Beauftragte für Datenschutz und Informationsfreiheit, Stellungnahme zum Gesetzentwurf zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 2**, S. 2.

Die gefährdeten Objekte können auch eine gesteigerte Grundrechtsrelevanz haben, wie zum Beispiel die Innenräume von Religionsstätten oder der Eingangsbereich von Redaktionsräumen,

vgl. Berliner Beauftragte für Datenschutz und Informationsfreiheit, Stellungnahme zum Gesetzentwurf zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 2**, S. 2.

Die Eingriffsintensität wird dadurch gesteigert, dass die Betroffenen der Videoüberwachung in vielen Fällen nicht ausweichen können, etwa wenn der Eingangsbereich zum Wohnhaus oder zum Arbeitsplatz erfasst ist. Personen, die auf der Straße leben oder sich wegen beengter Wohnverhältnisse viel im öffentlichen Raum aufhalten, sind in besonderem Maße von der Überwachung betroffen,

so auch der Sachverständige Dr. Philipp Knopp (TU Chemnitz) in der Sitzung des Ausschusses für Inneres, Sicherheit und Ordnung des Abgeordnetenhauses vom 1. Juni 2026, Wortprotokoll InnSichO 19/73, S. 9.

Unter Umständen sind sie einer ununterbrochenen Überwachung ausgesetzt, die weite Teile des Sozial- und Privatlebens erfasst (z.B. das Nächtigen in einem Park, der als kriminalitätsbelasteter Ort eingestuft ist).

Bei der Überwachung nach § 24 ASOG kommt hinzu, dass neben Bildaufzeichnungen auch Tonaufzeichnungen angefertigt werden können. Das kann auch Gespräche erfassen.

bb) Automatisierte Auswertung

Die automatisierte Auswertung hat ein gegenüber der Aufzeichnung gesteigertes Eingriffsgewicht.

Das Eingriffsgewicht einer automatisierten Auswertung ergibt sich zum einen aus dem Gewicht der vorausgegangenen Datenerhebungseingriffe. Zum anderen hat sie potenziell ein Eigengewicht, so dass weitergehende Rechtfertigungsanforderungen gelten,

vgl. BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19, 1 BvR 2634/20 –, Rn. 54.

Wie intensiv das Eigengewicht einer automatisierten Auswertung von Bild- und Tonaufzeichnungen ist, hängt maßgeblich von den technischen Modalitäten der Analyse ab,

vgl. Bäcker, Kriminalpräventionsrecht, 2015, S. 424.

Überträgt man die Kriterien, die das Bundesverfassungsgericht zur automatisierten Datenanalyse aufgestellt hat ((i)), auf die automatisierte Auswertung von Bild- und Tonaufzeichnungen, ergibt sich ein hohes Eingriffsgewicht ((ii)).

(i) Kriterien zur automatisierten Datenanalyse

Im Urteil vom 16. Februar 2023 – 1 BvR 1547/19 u.a. – hat das Bundesverfassungsgericht besondere Maßstäbe über den Zweckbindungsgrundsatz hinaus aufgestellt, um das Eingriffsgewicht einer automatisierten Datenanalyse zu bestimmen. Danach ist unter anderem zu berücksichtigen, ob die weitere Datenverarbeitung durch eine automatisierte Datenanalyse eigene Belastungseffekte haben

kann, die über das Eingriffsgewicht der ursprünglichen Erhebung hinausgehen,

vgl. BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19 –, Rn. 66 f.

Das Eingriffsgewicht wird vor allem durch Art und Umfang der verarbeitbaren Daten bestimmt. Je größere Mengen personenbezogener Daten in die automatisierte Datenanalyse und -auswertung einbezogen werden können, je weniger der Gesetzgeber also die verwendbare Datenmenge begrenzt, umso schwerer wiegt der Eingriff,

BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19 –, Rn. 78.

Eng mit der Regelung der Menge der verwendbaren Daten hängt auch die Regelung der Art der verwendbaren Daten zusammen. Je weniger die verwendbaren Daten der Art nach eingeschränkt sind, umso größer ist die zur Verarbeitung gelangende Datenmenge und umso höher ist tendenziell das Eingriffsgewicht. Die Art der Daten ist aber auch für sich genommen für das Eingriffsgewicht von Bedeutung, weil die Verwendung unterschiedlicher Daten direkt oder mittelbar unterschiedliche Persönlichkeitsrelevanz entfalten kann. Die Art und der Umfang der einbezogenen Daten und deren Auswirkungen auf das Gewicht des Grundrechtseingriffs können durch verschiedene Vorkehrungen näher bestimmt und beschränkt sein,

BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19 –, Rn. 78.

Eingriffsmildernd wirkt hingegen der Ausschluss der Verarbeitung von Daten, die ursprünglich durch besonders schwere Grundrechtseingriffe erlangt wurden. Darüber hinaus kann eine Regelung zugelassener Datenarten je nach der inhaltlichen Ausgestaltung begrenzende Wirkung entfalten. Das gilt auch für eine Regelung der einbeziehbaren Dateiformate, wie etwa von Bildern, Video- und Audioaufnahmen in die Datenanalyse oder -auswertung. Eingriffsmildernd kann etwa der Ausschluss biometrischer Daten wirken,

BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19 –, Rn. 81, 87.

Eingriffsverstärkend wirkt sich aus, je offener die Methode des Suchvorgangs gestaltet ist und je weniger die automatisierte Datenanalyse oder -auswertung durch – auch mit Erkenntnissen und Annahmen zu dem konkreten Sachverhalt gespeiste – polizeiliche Suchmuster gesteuert wird,

BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19 –, Rn. 93.

Das Eingriffsgewicht hängt zudem davon ab, welche Art von Suchergebnissen durch eine automatisierte Datenanalyse oder -auswertung erzielt wird. So ist das Eingriffsgewicht regelmäßig geringer, wenn die Datenanalyse oder -auswertung nicht auf personenbezogene Erkenntnisse, sondern etwa auf die Erkennung gefährlicher oder gefährdeter Orte zielt. Besonders eingriffsintensiv ist hingegen, wenn Ergebnis der automatisierten Anwendung personenbezogene Erkenntnisse sind und dieses Ergebnis maschinelle Sachverhaltsbewertungen enthält, die also über die bloße Anzeige von Übereinstimmungen zwischen dem Suchkriterium und den durchsuchten Daten hinausgehen. Eingriffsintensivierend ist insbesondere, wenn im Sinne eines „predictive policing“ maschinell Gefährlichkeitsaussagen über Personen getroffen werden,

BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19 –, Rn. 96 ff.

Besonders eingriffsintensiv ist auch, wenn sich das Verhalten einer Person, deren Gewohnheiten oder deren Lebensgestaltung räumlich und über längere Zeit hinweg nachvollziehen lassen, wenn also ein Bewegungs- oder Verhaltensprofil einer Person oder ein umfassenderes Persönlichkeitsbild entstehen kann,

BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19 –, Rn. 77.

Besonderes Eingriffsgewicht kann je nach Einsatzart die Verwendung lernfähiger Systeme, also KI, haben. Deren Mehrwert, zugleich aber auch ihre spezifischen Gefahren liegen darin, dass nicht nur von den einzelnen Polizistinnen und Polizisten aufgegriffene kriminologisch fundierte Muster Anwendung finden, sondern solche Muster automatisiert weiterentwickelt oder überhaupt erst generiert und dann in weiteren Analysestufen weiter verknüpft werden. Mittels einer automatisierten Anwendung könnten so über den Einsatz komplexer

Algorithmen zum Ausweis von Beziehungen oder Zusammenhängen hinaus auch selbstständig weitere Aussagen im Sinne eines „predictive policing“ getroffen werden. So könnten besonders weitgehende Informationen und Annahmen über eine Person erzeugt werden, deren Überprüfung spezifisch erschwert sein kann. Denn komplexe algorithmische Systeme könnten sich im Verlauf des maschinellen Lernprozesses immer mehr von der ursprünglichen menschlichen Programmierung lösen, und die maschinellen Lernprozesse und die Ergebnisse der Anwendung könnten immer schwerer nachzuvollziehen sein. Dann droht zugleich die staatliche Kontrolle über diese Anwendung verloren zu gehen,

vgl. BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19 –, Rn. 100.

Wird Software privater Akteure oder anderer Staaten eingesetzt, besteht zudem eine Gefahr unbemerkter Manipulation oder des unbemerkten Zugriffs auf Daten durch Dritte,

BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19, 1 BvR 2634/20 –, Rn. 100.

Der Einsatz von KI-Systemen ist auch eingriffsintensiv, da die Gefahr besteht, dass sich diskriminierende Algorithmen herausbilden,

vgl. BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19, 1 BvR 2634/20 –, Rn. 100.

Wie schwer Eingriffe durch automatisierte Datenanalyse oder -auswertung wiegen, hängt auch davon ab, wie fehleranfällig die eingesetzte Datenauswertungstechnologie ist und ob gegebenenfalls Vorkehrungen zur Entdeckung und Korrektur von Fehlern getroffen sind,

BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19 –, Rn. 102.

(ii) Übertragung auf die Auswertung von Bild- und Tonaufzeichnungen

Diese Kriterien sind auf die automatisierte Auswertung von Bild- und Tonaufzeichnungen zu übertragen,

vgl. Bäuerle, BeckOK PolR Hessen, 38. Ed. 1.4.2026, HSOG § 14 Rn. 53.

Eine hohe Eingriffsintensität ergibt sich daher zunächst aus Art und Umfang der Daten.

Die automatisierte Auswertung betrifft die Aufzeichnungen bei Veranstaltungen und Ansammlungen, gefährdeten Objekten und kriminalitätsbelasteten Orten. Sie betrifft damit eine Vielzahl von Orten und Personen. Es entsteht ein „flächendeckendes System automatisierter Verhaltensüberwachung“ das „nicht auf sog. ‚Angsträume‘ beschränkt“ ist, sondern dazu führen wird, „dass Unbeteiligte ihr Verhalten in der Öffentlichkeit anpassen und ggf. dennoch – aufgrund der zu erwartenden Fehleranfälligkeit – Ziel polizeilicher Maßnahmen werden“,

Berliner Beauftragte für Datenschutz und Informationsfreiheit, Stellungnahme zum Gesetzentwurf zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 2**, S. 7.

Auch ermächtigen die angegriffenen Normen keineswegs nur zu einer aufmerksamkeitsunterstützenden Live-Auswertung. Vielmehr nennt § 24e Abs. 4 Satz 1 ASOG die Auswertung der (gespeicherten) Bildaufzeichnungen ausdrücklich neben der Auswertung der (übertragenen) Bildaufnahmen. Die Vorschriften ermöglichen so die retrograde Auswertung gespeicherter Bildaufzeichnungen über einen Zeitraum von bis zu einem Monat bzw. zwei Monaten, in Einzelfällen sogar länger,

vgl. Berliner Beauftragte für Datenschutz und Informationsfreiheit, Stellungnahme zum Gesetzentwurf zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 2**, S. 6.

Auch handelt es sich bei den Videoaufnahmen und den Informationen von Verhaltensmustern um Daten, die nach § 42d für das KI-Training grundsätzlich weiterverwendet werden dürfen. Dies droht die Löschfristen zu unterlaufen, denn „Daten, die zum Training eines KI-Modells verwendet wurden, lassen sich schwerlich aus dem Modell entfernen“,

Berliner Beauftragte für Datenschutz und Informationsfreiheit, Stellungnahme zum Gesetzentwurf zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29

der Verfassung von Berlin, **Anlage 2**, S. 6; näher zum KI-Training unten V.

Auch die Methode der automatisierten Auswertung wirkt sich intensitätserhöhend aus.

Zwar begrenzt § 24e Abs. 4 Satz 2 ASOG die automatisierte Auswertung auf das Erkennen solcher Verhaltensmuster, die auf die Begehung einer Straftat oder den Eintritt eines Unglücksfalls im Sinne von § 323c Abs. 1 StGB hindeuten.

Es ist jedoch unklar, welche Straftaten und welche Unglücksfälle überhaupt durch eine Verhaltensmustererkennung erkannt werden sollen. Das Gesetz legt keine Verhaltensmuster fest,

näher dazu unten bb).

Auch ein „predictive policing“,

vgl. BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19, 1 BvR 2634/20, Rn. 90 ff.

ist nicht ausgeschlossen. Bezeichnend ist die inzwischen vorgenommenen Ausschreibung für die einzusetzende Technik. Danach ist etwa „langes Verharren oder Umhergehen ohne Anlass“ und „wiederholtes Erscheinen“ ein zu identifizierendes Verhalten,

siehe oben und Polizei Berlin, Leistungsverzeichnis Projekt zur Erprobung KI-gestützter Videotechnik im Objektschutz der Polizei Berlin, **Anlage 8**, S. 7.

Ein „langes Verharren oder Umhergehen ohne Anlass“ ist keine Straftat, sondern ein legales und sozialadäquates Verhalten. Die Polizei scheint dieses „atypische“ Verhalten jedoch als Indiz dafür zu sehen, dass die Person in Zukunft eine Straftat begehen wird, beziehungsweise eine entsprechende Absicht hat.

Das Beispiel des wiederholten Erscheinens zeigt zudem, dass das Verhalten bestimmter Personen an bestimmten Orten umfassend und über einen längeren Zeitraum nachvollzogen und ausgewertet werden kann,

vgl. zum Eingriffsgewicht BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19, 1 BvR 2634/20 –, Rn. 77; Bäcker, Kriminalpräventionsrecht, 2015, S. 425.

Die Begrenzungen der Methoden in § 24e Abs. 4 Satz 3 ASOG tragen nicht merklich zur Reduzierung des Eingriffsgewichts bei. Der vermeintliche Ausschluss autonomer Entscheidungen in § 24e Abs. 4 Satz 3 ASOG verlagert die Entscheidung über Maßnahmen zwar formal zurück auf den Menschen, ändert aber nichts daran, dass die algorithmische Vorauswahl den Wahrnehmungs- und Entscheidungsspielraum der Beamtinnen und Beamten faktisch beeinflussen kann und wird (sogenannter Automation Bias),

vgl. allgemein zum Automation Bias: European Crime Prevention Network (EUCPN), Artificial Intelligence and predictive policing: Risks and challenges, 2022, <https://eucpn.org/sites/default/files/document/files/PP%20%282%29.pdf>, S. 12.

Es besteht „die Gefahr, dass auch gut eingestellte ‚Assistenzsystem‘ in der Praxis den Spielraum möglicher Handlungen der Beamt:innen so weit einschränken, dass eine ‚Unterstützung‘ von einer ‚Entscheidung‘ nicht mehr zu unterscheiden ist“,

Weizenbaum-Institut, Stellungnahme zur Novellierung des Allgemeinen Sicherheits- und Ordnungsgesetzes Berlin (ASOG Bln), Policy Paper #19, März 2026, S. 14, 15 f.

Zwar verbietet § 24e Abs. 4 Satz 3 ASOG eine automatisierte biometrische Fernidentifizierung sowie die Nutzung der Bildaufnahmen und -aufzeichnungen für das Testen oder Trainieren von Programmen zur biometrischen Fernidentifizierung. Die Norm ist ansonsten jedoch methodenoffen ausgestaltet und schließt den Einsatz – auch selbstlernender – künstlicher Intelligenz nicht aus,

vgl. Berliner Beauftragte für Datenschutz und Informationsfreiheit, Stellungnahme zum Gesetzentwurf zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 2**, S. 6.

Das begründet die Gefahr, dass Verhalten als gefährlich erkannt wird, ohne dass dies menschlich nachvollzogen werden kann.

Der Ausschluss der „automatisierten biometrischen Fernidentifizierung“ in § 24e Abs. 4 Satz 3 ASOG hat auch nicht zur Folge, dass keine biometrischen Daten ausgewertet werden können. Denn der Ausschluss bezieht sich nur auf die „automatisierte“ biometrische Fernidentifizierung. Eine manuelle Fernidentifizierung ist nach § 24e Abs. 4 ASOG zulässig.

Es besteht ein erhebliches Diskriminierungsrisiko,

vgl. BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19, 1 BvR 2634/20, Rn. 100.

So können insbesondere Bewegungen von Menschen mit Behinderungen oder Wohnungslose von dem Algorithmus als auffällig bewertet werden,

vgl. Sußner, Try harder hilft selten: Eine verfassungsrechtliche Einordnung der Videoüberwachung an kriminalitätsbelasteten Orten, Verfassungsblog vom 8. Januar 2026, <https://verfassungsblog.de/berlin-asog-novelle-kbos/>.

Gleiches gilt für andere Personengruppen wie Menschen mit Abhängigkeitserkrankungen oder Kinder und Jugendliche, deren Verhalten „atypisch“ sein kann.

Schutzvorkehrung gegen diskriminierende Algorithmen sind nicht getroffen worden,

näher dazu unten ee).

Schließlich ist das System fehleranfällig,

vgl. BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19, 1 BvR 2634/20 –, Rn. 102.

Die bisherigen Versuche mit Verhaltenserkennung belegen eine hohe Fehleranfälligkeit,

siehe oben 2. und Weizenbaum-Institut, Stellungnahme zur Novellierung des Allgemeinen Sicherheits- und Ordnungsgesetzes Berlin (ASOG Bln), Policy Paper #19, März 2026, S. 15 f.

Auch die Polizei Berlin geht in ihrer Ausschreibung von einer hohen Falsch-Positiv-Rate von bis zu 5 % aus,

siehe oben 2. und Anlage A.2.1 – Anforderungskatalog, **Anlage 10**, S. 10.

Gesetzgeberische Schutzvorkehrungen gegen fehlerhafte Verdachtsmeldungen hat der Gesetzgeber nicht getroffen,

näher dazu unten ee).

b) Verletzung der verfassungsrechtlichen Anforderungen

Aus dem jeweiligen Eingriffsgewicht folgen spezifische Anforderungen an die Rechtfertigung der Grundrechtseingriffe. Die angegriffenen Vorschriften verletzen diese Anforderungen.

Sie enthalten keine hinreichend gehaltvollen Voraussetzungen (aa)) und legen die zu erkennenden Verhaltensmuster nicht fest (bb)). Zudem fehlt es an einer ausreichenden Pflicht zur Kenntlichmachung (cc)), an einer ausreichenden Dokumentationspflicht (dd)) und an Schutzvorkehrungen gegen Fehler, Diskriminierung und Missbrauch (ee)).

aa) Unzureichende Voraussetzungen

Wegen der gehobenen Eingriffsintensität setzt die Aufzeichnung voraus, dass der überwachte Ort eine Schadensdisposition aufweist, die ihn quantitativ und qualitativ heraushebt. Für die Überwachung „gefährlicher Orte“ folgt daraus etwa, dass es sich um einen Kriminalitätsbrennpunkt handeln muss, an dem bestimmte Straftaten besonders häufig begangen werden. Diese Straftaten müssen zumindest der mittleren Kriminalität zuzuordnen sein,

Bäcker, Kriminalpräventionsrecht, 2015, S. 424.

Die automatisierte Auswertung verlangt wegen der gesteigerten Eingriffsintensität gegenüber der bloßen Aufzeichnung gesteigerte Eingriffsvoraussetzungen. Der Ort oder die Situation muss sich daher durch eine erhöhte Schadensdisposition auszeichnen, etwa indem auf die Begehung schwerer Straftaten abgestellt wird. Die gezielte Überwachung einer bestimmten Person ist nur zulässig, wenn diese für eine mindestens konkretisierte Gefahr verantwortlich ist,

vgl. Bäcker, Kriminalpräventionsrecht, 2015, S. 425.

Die angegriffenen Vorschriften verfehlen diese Anforderungen, auch weil sie keine gesteigerten Anforderungen an die automatisierte Auswertung stellen. Das gilt für die Überwachung bei Veranstaltungen und Ansammlungen ((i)), an und in gefährdeten Objekten ((ii)) sowie an kriminalitätsbelasteten Orten ((iii)).

(i) Veranstaltungen und Ansammlungen

Die Videoüberwachung bei Veranstaltungen und Ansammlungen ist nach § 24 Abs. 1 Satz 1 ASOG bereits zulässig, wenn Tatsachen die Annahme rechtfertigen, dass dabei Straftaten begangen werden. Eine Einschränkung auf erhebliche Straftaten wie bei den kriminalitätsbelasteten Orten fehlt (anders als etwa in § 32 Abs. 3 Nr. 2 BremPolG). Nach dem Wortlaut genügt damit der Verdacht, dass Bagatelldelicten begangen werden.

Erforderlich ist auch kein besonderes Gefährdungsrisiko (anders als etwa in § 44 PolG BW), in dem Sinne, dass bei der Veranstaltung oder Ansammlung eine erhöhte Gefahr von Straftaten besteht. Damit kann praktisch jede größere Veranstaltung überwacht werden, denn überall, wo Menschen zusammenkommen, rechtfertigen Tatsachen die Annahme, dass Straftaten begangen werden.

Diese Schwelle genügt schon nicht den Anforderungen an die Rechtfertigung von Bild- und Tonaufzeichnungen. Jedenfalls für die automatisierte Auswertung verfehlt die Eingriffsschwelle die verfassungsrechtlichen Anforderungen.

(ii) Gefährdete Objekte

Nach § 24a Abs. 1 Satz 1 ASOG sind Bildaufzeichnungen zulässig, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass an oder in einem Objekt dieser Art Straftaten drohen. Die Norm knüpft ebenfalls an jegliche Straftaten an.

Die Gefährdungsbewertung basiert zudem im Wesentlichen auf der „Art“ des Objekts. Auf die tatsächlichen Gegebenheiten vor Ort kommt es nicht an,

vgl. Berliner Beauftragte für Datenschutz und Informationsfreiheit, Stellungnahme zum Gesetzentwurf zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 2**, S. 1.

Beim Vergleich mit § 24 Abs. 1 Satz 1 ASOG fällt zudem auf, dass § 24a Abs. 1 Satz 1 ASOG nur „tatsächliche Anhaltspunkte“ (statt Tatsachen) verlangt und diese lediglich die Annahme rechtfertigen müssen, dass Straftaten „drohen“ (statt begangen werden). Die Eingriffsschwelle verliert dadurch weiter an Kontur.

Beispielsweise dürfte bei den meisten Gebäuden tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass dort Sachbeschädigungen (z.B. Graffiti) drohen. Selbst wenn man den Tatbestand auf bestimmte Arten von Gebäuden begrenzt (z.B. Brücken, Gebäude mit zugänglichen Außenwänden) könnten weite Teile der Stadt überwacht werden. Das ist nicht mehr verhältnismäßig.

Dies gilt erst recht für die automatisierte Auswertung, die gemäß § 24a Abs. 1 Satz 2 ASOG keinen höheren Voraussetzungen unterliegt.

Das Bundesverfassungsgericht hat zwar ähnliche Formulierungen für die Kennzeichenerfassung gebilligt,

BVerfGE 150, 244 <292 Rn. 123>; 150, 309 <338 Rn. 78>.

Die Kennzeichenerfassung hat jedoch nicht die gleiche Eingriffsintensität, da es sich beim Kennzeichen nur um ein mittelbar personenbezogenes Datum handelt und die Aufnahmen im Falle eines Nicht-Treffers sofort gelöscht werden,

BVerfGE 150, 244 <283 Rn. 97>.

(iii) Kriminalitätsbelastete Orte

§ 24e Abs. 1 Satz 1 ASOG ermächtigt zur Aufzeichnung von Bildern an kriminalitätsbelasteten Orten. Diese werden gemäß § 17a Abs. 1 Satz 1 ASOG in der Regel durch Rechtsverordnung festgelegt. Dies ist nur für solche Orte zulässig, die öffentlich zugänglich sind und von denen Tatsachen die Annahme rechtfertigen, dass dort Personen Straftaten von erheblicher Bedeutung verabreden, vorbereiten oder verüben (§ 17a Abs. 1 Satz 2 ASOG).

Hier erfolgt zwar eine Beschränkung auf Straftaten von erheblicher Bedeutung. Die Norm setzt jedoch nicht voraus, dass sich die Schadensdisposition auch quantitativ abhebt. Erforderlich ist auch nicht, dass bereits wiederholt Straftaten begangen wurden oder die

Beschaffenheit des Ortes die Begehung von Straftaten begünstigt (anders als etwa in § 15a Abs. 1 Nr. 1 PolG NRW).

Nach dem Wortlaut ist der Tatbestand an nahezu allen Orten Berlins erfüllt: Wo sich Menschen aufhalten, werden Straftaten (auch solche von erheblicher Bedeutung) verabredet, vorbereitet oder verübt. Dies steht jedoch in Widerspruch zum Verhältnismäßigkeitsgrundsatz. Eine solche „Durchführung von Kontrollen zu beliebiger Zeit und an beliebigem Ort ins Blaue hinein“ ist mit dem Rechtsstaatsprinzip grundsätzlich unvereinbar,

BVerfG, Beschluss des Ersten Senats vom 18. Dezember 2018 – 1 BvR 142/15 –, Rn. 92.

Das Bundesverfassungsgericht hat daher in seiner Entscheidung zur Kennzeichenerfassung in Bayern eine vergleichbare Norm einschränkend ausgelegt:

„Bei verständiger Auslegung der Vorschrift im Lichte des Verhältnismäßigkeitsgrundsatzes bestehen gegen die Vorschrift keine durchgreifenden Bedenken. [...]

Die Regelung knüpft dabei nicht an eine bloß abstrakte Gefährlichkeit bestimmter Orte an, sondern begrenzt die Kontrollen auf Orte, für die tatsächliche Anhaltspunkte bestehen, dass sie von den in der Vorschrift genannten Personen maßgeblich frequentiert werden. Sie enthält damit nicht etwa eine Generalermächtigung für Kennzeichenkontrollen an praktisch allen wichtigen Verkehrsknotenpunkten oder Orten größerer Zusammenkünfte von Menschen. Vielmehr muss es sich um Orte handeln, für die in diesem Sinne konkrete Erkenntnisse der Polizei vorliegen.“

BVerfG, Beschluss des Ersten Senats vom 18. Dezember 2018 – 1 BvR 142/15 –, Rn. 119 f.

Auch in der fachgerichtlichen Rechtsprechung zu vergleichbaren Landesgesetzen wird eine einschränkende Auslegung vertreten. So verlangt der Verwaltungsgerichtshof Baden-Württemberg für Videoüberwachung an „gefährlichen Orten“, dass

„die Örtlichkeit eine besondere Kriminalitätsbelastung aufweisen, es sich bei ihr um einen sog. Kriminalitätsbrennpunkt handeln muss. Die Annahme eines Kriminalitätsbrennpunktes setzt dabei grundsätzlich voraus, dass sich die Kriminalitätsbelastung des Ortes deutlich von der an anderen Orten abhebt. Dabei geht der Senat davon aus, dass

die Vergleichsorte innerhalb derselben Stadt liegen müssen, da die Überwachung nach ihrer Zweckrichtung den besonderen örtlichen Gefahrenschwerpunkten gilt und damit einen örtlichen Bezug hat (vgl. Waechter, NdsVBl 2001, 77, 83).“

Verwaltungsgerichtshof Baden-Württemberg, Urteil vom 21. Juli 2003 – 1 S 377/02 –, Rn. 60.

Auch das Oberverwaltungsgericht Nordrhein-Westfalen legt die Voraussetzungen eines „gefährlichen Ortes“ einschränkend aus. Aus dem Verhältnismäßigkeitsgrundsatz ergebe sich, dass eine Videoüberwachung nur an Kriminalitätsschwerpunkten zulässig sei. Zur Ermittlung eines Kriminalitätsschwerpunktes sei regelmäßig eine vergleichende Betrachtung der Straßenkriminalitätsbelastung an dem überwachten bzw. zu überwachenden Ort mit derjenigen im gesamten Gebiet einer Stadt bzw. Gemeinde vorzunehmen

Oberverwaltungsgericht für das Land Nordrhein-Westfalen, Beschluss vom 16. Mai 2022 – 5 B 137/21 –, Rn. 96 ff.

Das Verwaltungsgericht Berlin hat hingegen in einer Entscheidung von 2017 entschieden, dass es auf „einen Vergleich mit anderen Orten im Land Berlin, in der Weise, dass Maßnahmen i.S.d. § 21 Abs. 2 Nr. 1 a) aa) ASOG nur an dem/den jeweils gefährlichsten Ort(en) zulässig wären oder eine bestimmte Häufigkeit von erheblichen Straftaten zu fordern wäre“ nicht ankomme,

VG Berlin, Urteil vom 15. September 2017 – 1 K 759.16 –, Rn. 22; bestätigt durch Oberverwaltungsgericht Berlin-Brandenburg, Beschluss vom 28. Juni 2018 – OVG 1 N 98.17 –, Rn. 8.

Trotz dieser Rechtsprechung hat der Gesetzgeber die bisherige Formulierung aus § 21 Abs. 2 Nr. 1 a) aa) ASOG a.F. in § 17a Abs. 1 Satz 2 ASOG übernommen und zur Grundlage für Videoüberwachung gemacht,

Abgh-Drs. 19/2553, S. 144.

Die Bestimmung ist daher einer verfassungskonformen Auslegung nicht zugänglich.

Die automatisierte Auswertung der Daten unterliegt nach § 24e Abs. 4 ASOG keinen erhöhten Voraussetzungen und ist daher erst recht verfassungswidrig.

bb) Fehlende Festlegung der Verhaltensmuster

Es muss zudem im Gesetz festgelegt werden, welche Verhaltensmuster erkannt werden sollen. Hierbei handelt es sich um eine grundrechtswesentliche Frage. Insbesondere steigt die Gefahr von Fehlprognosen, wenn hochgradig interpretationsbedürftiges oder sozialadäquates Verhalten wie das „lange Verweilen“ als Hinweis auf eine Straftat gewertet wird,

siehe dazu oben 2.

Eine transparente Regelung kann zudem besondere „chilling effects“ vermeiden, die dadurch entstehen, dass Personen nicht erraten können, welches Verhalten möglicherweise als gefährlich erkannt wird. Zumindest sind die Verhaltensmuster in einer Verwaltungsvorschrift zu benennen und bekanntzumachen,

vgl. BVerfGE 165, 363 <414 Rn. 113>.

Die angegriffenen Vorschriften enthalten keine solchen Vorgaben. § 24e Abs. 4 Satz 1 ASOG bezieht sich auf Verhaltensmuster, „die auf die Begehung einer Straftat oder den Eintritt eines Unglücksfalls im Sinne von § 323c Absatz 1 des Strafgesetzbuches hindeuten“. Es wird nicht konkretisiert, welche Verhaltensmuster das sein können. Auch eine zu veröffentlichende Verwaltungsvorschrift ist – anders als nach § 28a Abs. 6 ASOG – nicht vorgesehen. Anhaltspunkte lassen sich lediglich der Ausschreibung entnehmen, die nicht öffentlich ist und keine verbindlichen Vorgaben macht,

siehe oben 2.

cc) Fehlende Kenntlichmachung

Der Verhältnismäßigkeitsgrundsatz stellt zudem Anforderungen an Transparenz und individuellen Rechtsschutz. So ist die Videoüberwachung und die automatisierte Auswertung in geeigneter Form kenntlich zu machen. Erst die offene Datenerhebung bewirkt nämlich, dass die Betroffenen von der Datenerhebung Kenntnis

erhalten und ihr Recht auf informationelle Selbstbestimmung wahrnehmen können,

Oberverwaltungsgericht für das Land Nordrhein-Westfalen,
Beschluss vom 23. September 2022 – 5 B 303/21 –, Rn. 124.

Um ihrer Funktion insbesondere in verfassungsrechtlicher Hinsicht gerecht werden zu können, müssen Hinweisschilder so aufgestellt sein, dass jede Person, die sich dem videoüberwachten Bereich nähert, diesen bereits vor dem Betreten als solchen erkennen kann.

Oberverwaltungsgericht für das Land Nordrhein-Westfalen,
Beschluss vom 23. September 2022 – 5 B 303/21 –, Rn. 131.

Auf eine Kennzeichnung darf nur verzichtet werden, wenn die Überwachung offenkundig ist. Dabei ist wegen des Rechts auf informationelle Selbstbestimmung ein strenger Maßstab anzulegen,

Oberverwaltungsgericht für das Land Nordrhein-Westfalen,
Beschluss vom 23. September 2022 – 5 B 303/21 –, Rn. 124.

Nach § 24 Abs. 1 Satz 3 ASOG sind zwar verdeckte Bild- und Tonaufzeichnungen unzulässig. Eine explizite Hinweis- oder Kennzeichnungspflicht gibt es jedoch bei der Datenerhebung bei öffentlichen Veranstaltungen und Ansammlungen nicht.

§ 24a Abs. 2 und § 24e Abs. 2 Satz 2 ASOG enthalten zwar eine solche Pflicht. Diese bezieht sich jedoch nur auf den Umstand der Beobachtung und Aufzeichnung, nicht auf die automatisierte Auswertung. § 24e Abs. 4 Satz 5 ASOG erklärt nur § 24e Abs. 2 Satz 1 ASOG, nicht § 24e Abs. 2 Satz 2 ASOG für entsprechend anwendbar. Damit fehlt es an einer Kennzeichnungs- oder Hinweispflicht für die automatisierte Auswertung. Betroffene können nicht absehen, wo ihr Verhalten automatisiert zur Verdachtsgenerierung ausgewertet wird. Dies erhöht die damit verbundenen „chilling effects“ und ist unverhältnismäßig.

dd) Unzureichende Dokumentationspflicht

Die Aufzeichnungen und deren Auswertungen sind zudem nur dann verhältnismäßig, wenn die Entscheidungsgrundlagen nachvollziehbar und überprüfbar dokumentiert werden,

vgl. BVerfGE 150, 244 <303 Rn. 157> zur Kennzeichenerfassung;
SächsVerfGH, Urteil vom 10. Juli 2013 – Vf. 43-II-00 –, juris, Rn. 218
ff. zu Identitätsfeststellungen.

Dies ist von dreifacher Bedeutung: Zum einen rationalisiert und mäßigt es die Entscheidung der Behörde selbst, wenn diese sich über ihre Entscheidungsgrundlagen Rechenschaft ablegen muss. Zum anderen ermöglicht die Dokumentation erst eine aufsichtliche Kontrolle durch die Datenschutzbeauftragte. Schließlich wird damit die verwaltungsgerichtliche Kontrolle erleichtert,

vgl. BVerfGE 150, 244 <303 Rn. 157> zur Kennzeichenerfassung;
SächsVerfGH, Urteil vom 10. Juli 2013 – Vf. 43-II-00 –, juris, Rn. 218
ff. zu Identitätsfeststellungen.

Eine zu dokumentierende Anordnung ist nach § 24e Abs. 2 Satz 1 ASOG nur für die Datenerhebung an kriminalitätsbelasteten Orten und nach § 24e Abs. 4 Satz 5 ASOG für die automatisierte Auswertung vorgesehen. Für die Datenerhebung bei öffentlichen Veranstaltungen und Ansammlungen sowie an und in gefährdeten Objekten fehlt es an einer zu dokumentierenden Anordnung. Zudem ist in § 24e Abs. 2 Satz 1 ASOG nur vorgesehen, dass die Anordnung dokumentiert wird. Im Unterschied zu § 27c ASOG hat der Gesetzgeber den Inhalt der Dokumentationspflicht nicht besonders ausgestaltet. Eine Begründungspflicht besteht nicht, sodass nicht sichergestellt ist, dass die Entscheidungsgrundlagen für die Datenerhebung und -auswertung nachvollziehbar und überprüfbar dokumentiert sind,

vgl. Weizenbaum-Institut, Stellungnahme zur Novellierung des Allgemeinen Sicherheits- und Ordnungsgesetzes Berlin (ASOG Bln), Policy Paper #19, März 2026, S. 17.

ee) Fehlende Vorkehrungen gegen Fehler, Diskriminierung und Datenmissbrauch

Wird Software eingesetzt, die komplexere Formen des automatisierten Abgleichs von Daten erlaubt, sind auch Vorkehrungen gegen eine hiermit spezifisch verbundene Fehleranfälligkeit erforderlich, was auch gesetzliche Regelungen zu einem staatlichen Monitoring der Entwicklung der eingesetzten Software erfordern kann,

BVerfG Urteil vom 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 –, Rn. 109.

Zur Verhinderung diskriminierender Systeme dürfen selbstlernende Systeme in der Polizeiarbeit zudem nur unter besonderen verfahrensrechtlichen Vorkehrungen zur Anwendung kommen, die trotz der eingeschränkten Nachvollziehbarkeit ein hinreichendes Schutzniveau sichern,

BVerfG Urteil vom 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 –, Rn. 100.

Wird die Nutzung einer Software privater Akteure oder anderer Staaten nicht ausgeschlossen, sind zudem Schutzvorkehrungen gegen Manipulation oder Datenzugriffe durch Dritte erforderlich,

vgl. BVerfG Urteil vom 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 –, Rn. 100; Kelber/Bortnikov, NJW 2023, 2000.

Erforderlich wären etwa „regelmäßige externe Audits, die Offenlegung von Trainingsdaten und Algorithmen, soweit datenschutzrechtlich und geheimnisschutzrechtlich zulässig sowie klare Verantwortlichkeiten für Fehlalarme und Diskriminierungseffekte“,

Weizenbaum-Institut, Stellungnahme zur Novellierung des Allgemeinen Sicherheits- und Ordnungsgesetzes Berlin (ASOG Bln), Policy Paper #19, März 2026, S. 17.

Zudem müssten Vorgaben zur Qualität der Trainings- oder Testdaten gemacht werden,

vgl. Kühne/Golla/Schäfer, GSZ 2025, 272 (281); Hüger, Künstliche Intelligenz und Diskriminierung, 2023, S. 158 ff. m.w.N.; Lauscher/Legner, ZfDR 2022, 367 (371).

An solchen Schutzvorkehrungen fehlt es vorliegend.

§ 12 Abs. 3 ASOG enthält lediglich einen deklaratorischen Verweis auf allgemeine Diskriminierungsverbote,

vgl. Sußner, Try harder hilft selten: Eine verfassungsrechtliche Einordnung der Videoüberwachung an kriminalitätsbelasteten Orten, Verfassungsblog vom 8. Januar 2026, <https://verfassungsblog.de/berlin-asog-novelle-kbos/>,

und keine konkreten Vorgaben für selbstlernende Systeme.

Anders als in § 42d Abs. 1 Satz 2 ASOG und § 47a Abs. 1 Satz 6 ASOG wurde in § 24e Abs. 4 ASOG nicht einmal eine Klausel eingefügt, nach der sicherzustellen ist, dass diskriminierende Algorithmen weder herausgebildet noch verwendet werden. Ein Training oder eine Testung des Systems nach § 42d ASOG ist nicht verpflichtend vorgeschrieben,

vgl. Aden et al, vorgänge. Zeitschrift für Bürgerrechte und Gesellschaftspolitik Nr. 253 [65(1)], S. 177 (184).

Abgesehen davon enthält § 42d Abs. 1 Satz 2 ASOG keine hinreichend konkreten Vorgaben. Die Formulierung, wonach bei der Weiterverarbeitung sicherzustellen ist, dass diskriminierende Algorithmen weder herausgebildet noch verwendet werden, ist ein „legislatives Lippenbekenntnis“,

vgl. Lenschow, Allwissende Polizei?: Entgrenzungen im Polizeirecht durch intelligente Gefahrenermittlung am Beispiel des SächsPVDG-E, Verfassungsblog vom 7. Januar 2026, <https://verfassungsblog.de/polizeigesetz-sachsen-referentenentwurf/>.

Wie genau ein solches algorithmisches Diskriminierungsverbot faktisch durchgesetzt werden soll, bleibt offen,

vgl. Berliner Beauftragte für Datenschutz und Informationsfreiheit, Stellungnahme zum Änderungsantrag der Fraktion der CDU und der Fraktion der SPD zur Drucksache 19/2553: Gesetz zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 7**, S. 5; Bäuerle, in: BeckOK PolR Hessen, 39. Ed. 1.7.2026, HSOG § 25a Rn. 138; Arzt, in: BeckOK PolR NRW/Arzt, 34. Ed. 15.4.2026, PolG NRW § 23 Rn. 82.

Auch die Gesetzgebung lässt eine Auseinandersetzung mit Diskriminierungspotential der Verhaltenserkennung gänzlich vermissen.

Es fehlt zudem an Schutzvorkehrungen gegen Manipulation oder Datenzugriffe. Das Gesetz enthält keine Vorschriften dazu, welche Software eingesetzt wird. Es wird insbesondere nicht ausgeschlossen, dass Software von privaten Dritten angewendet wird und diese Zugriff auf die Daten erhalten. Zudem fehlt es gänzlich an darauf bezogenen Schutzvorkehrungen, wie sie z.B. § 42d Abs. 3 ASOG vorsieht.

Schutzvorkehrungen müssten zumindest in einer zu veröffentlichenden Verwaltungsvorschrift (vgl. § 42d Abs. 4 ASOG) festgelegt werden.

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

Die §§ 26a, 26b ASOG verstoßen gegen das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 7 i.V.m. Art. 6 VvB oder Art. 33 VvB, sowie gegen das Fernmeldegeheimnis aus Art. 16 VvB.

Die Normen enthalten Befugnisse zur Quellen-Telekommunikationsüberwachung und Online-Durchsuchung (1.). Beide Maßnahmen beinhalten die Infiltration informationstechnischer Systeme mittels eines sogenannten Staatstrojaners, was regelmäßig die Ausnutzung von IT-Schwachstellen voraussetzt (2.).

Das greift in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme sowie in das Fernmeldegeheimnis ein (3.). Diese Eingriffe sind nicht gerechtfertigt (4.). Angesichts ihrer außerordentlichen Eingriffsintensität (4. a)) genügen die gesetzlichen Voraussetzungen den verfassungsrechtlichen Anforderungen nicht. Die Vorschriften schützen teilweise keine hinreichend gewichtigen Rechtsgüter (4. b) aa)), unterschreiten die verfassungsrechtlich gebotenen Eingriffsschwellen (4. b) bb)) und enthalten eine unzulässige dynamische Verweisung auf Bundesrecht (4. b) cc)). Darüber hinaus fehlen gesetzliche Regelungen zur Überprüfung der eingesetzten Software (4. c)) und zum Umgang mit den für den Einsatz von Staatstrojanern erforderlichen IT-Schwachstellen (4. d)).

1. Gesetz und Gesetzesbegründung

§ 26a ASOG ermächtigt zur Datenerhebung durch Telekommunikationsüberwachung informationstechnischer Systeme (sogenannte Quellen-Telekommunikationsüberwachung). § 26b ASOG ermächtigt zur Datenerhebung durch verdeckten Eingriff in informationstechnische Systeme (sogenannte Online-Durchsuchung).

Die Normen haben folgenden Wortlaut:

§ 26a

Datenerhebung durch Telekommunikationsüberwachung informationstechnischer Systeme

(1) Maßnahmen nach § 26 Absatz 1 können in der Weise erfolgen, dass mit technischen Mitteln in von den genannten Personen genutzte informationstechnische Systeme eingegriffen wird, wenn

1. Tatsachen die Annahme rechtfertigen, dass die Person innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise

a) eine terroristische Straftat oder

b) eine in § 100b Absatz 2 der Strafprozessordnung genannte und voraussichtlich auch im Einzelfall besonders schwerwiegende Straftat organisiert, insbesondere banden-, gewerbs- oder serienmäßig,

begehen oder an ihr teilnehmen wird,

2. das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums eine terroristische Straftat begehen oder an ihr teilnehmen wird, oder

3. Tatsachen die Annahme rechtfertigen, dass

a) die Person Mitteilungen, die für eine in den Nummern 1 oder 2 genannte Person bestimmt sind oder die von dieser herrühren, entgegennimmt oder weitergibt, oder

b) der Telekommunikationsanschluss oder das Endgerät der Person von einer in den Nummern 1 oder 2 genannten Person genutzt wird,

und der Eingriff notwendig ist, um die Telekommunikation insbesondere in unverschlüsselter Form überwachen und aufzeichnen zu können.

(2) Es ist technisch sicherzustellen, dass

1. ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird,

2. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind, und

3. die vorgenommenen Veränderungen bei Beendigung der Maßnahme, soweit technisch möglich, automatisiert rückgängig gemacht werden.

Das eingesetzte Mittel ist nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. Kopierte Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen.

(3) Soweit dies zur Durchführung der Maßnahme erforderlich ist, sind verdeckte Durchsuchungen von Sachen sowie das verdeckte Betreten und Durchsuchen von Räumlichkeiten der betroffenen Personen zulässig. Hierfür gilt § 26 Absatz 2 entsprechend.

§ 26b

Datenerhebung durch verdeckten Eingriff in informationstechnische Systeme

(1) Unter den gleichen Voraussetzungen wie in § 26a Absatz 1 kann die Polizei durch den verdeckten Einsatz technischer Mittel in von einer in § 26a Absatz 1

Nummer 1 oder 2 genannten Person genutzte informationstechnische Systeme eingreifen und aus ihnen Daten erheben.

(2) In informationstechnische Systeme anderer Personen darf die Maßnahme nur eingreifen, wenn Tatsachen die Annahme rechtfertigen, dass eine in § 26a Absatz 1 Nummer 1 oder 2 genannte Person dort relevante Informationen speichert, und die Maßnahme zur Abwehr der Gefahr oder zur Verhütung der Straftat unerlässlich ist.

(3) Die Maßnahme ist nur zulässig, wenn die Abwehr der Gefahr oder die Verhütung der Straftat auf andere Weise aussichtslos oder wesentlich erschwert wäre; sie darf nicht außer Verhältnis zur Bedeutung des aufzuklärenden Sachverhalts stehen. Die Maßnahme darf auch durchgeführt werden, wenn andere Personen unvermeidbar betroffen werden.

(4) Soweit dies zur Durchführung der Maßnahme erforderlich ist, kann die Polizei unter den dort genannten Voraussetzungen technische Mittel einsetzen, um erforderliche Verkehrsdaten, insbesondere spezifische Kennungen oder Standortdaten eines informationstechnischen Systems, zu erheben. Personenbezogene Daten Dritter dürfen dabei nur erhoben werden, wenn dies aus technischen Gründen unvermeidbar ist. Nach Beendigung der Maßnahme sind diese personenbezogenen Daten Dritter unverzüglich zu löschen. Die Löschung ist zu dokumentieren.

(5) Soweit dies zur Durchführung der Maßnahme erforderlich ist, sind verdeckte Durchsuchungen von Sachen sowie das verdeckte Betreten und Durchsuchen von Räumlichkeiten der betroffenen Personen zulässig.

(6) Die Maßnahmen nach den Absätzen 1 bis 5 bedürfen der gerichtlichen Anordnung, die von der Polizeipräsidentin oder dem Polizeipräsidenten oder der Vertretung im Amt zu beantragen ist. Bei Gefahr im Verzug kann die Anordnung durch die Polizeipräsidentin oder den Polizeipräsidenten oder die Vertretung im Amt getroffen werden. Die gerichtliche Bestätigung der Anordnung ist in diesem Fall unverzüglich einzuholen. Die Anordnung tritt außer Kraft, wenn sie nicht binnen drei Werktagen gerichtlich bestätigt wird. In diesem Fall dürfen die bereits erhobenen Daten nicht mehr verwendet werden; sie sind unverzüglich zu löschen. Sind bereits Daten übermittelt worden, die nach Satz 5 zu löschen sind, so ist die empfangende Stelle darüber zu unterrichten.

(7) Die Anordnung ist auf höchstens einen Monat zu befristen. Eine Verlängerung um jeweils nicht mehr als einen weiteren Monat ist auf Antrag zulässig, soweit die Voraussetzungen der Anordnung fortbestehen. Liegen die Voraussetzungen der Anordnung nicht mehr vor, ist die Maßnahme unverzüglich zu beenden.

(8) Sämtliche mit einer Maßnahme nach Absatz 1 erhobenen personenbezogenen Daten sind dem anordnenden Gericht unverzüglich vorzulegen und dürfen bis zu der Entscheidung des Gerichts nicht verwendet werden. Das Gericht entscheidet unverzüglich über die Verwertbarkeit oder Löschung dieser Daten zum Schutz des Kernbereichs privater Lebensgestaltung nach § 27a Absatz 1 und 3 sowie zum Schutz zeugnisverweigerungsberechtigter Berufsheimnisträgerinnen und Berufsheimnisträger nach § 18a; es unterrichtet die Polizei unverzüglich über den Inhalt der verwertbaren Daten. § 27a Absatz 5 gilt entsprechend.

(9) § 26 Absatz 4 und § 26a Absatz 2 Satz 1 Nummer 2 und 3 sowie Satz 2 und 3 gelten entsprechend.

Die Einführung der Quellen-Telekommunikationsüberwachung in § 26a ASOG wurde damit begründet, dass Kriminelle ihre Telekommunikation inzwischen größtenteils über verschlüsselte Verbindungen führen würden. Die Aufklärung verschlüsselter Telekommunikation setze voraus, dass diese noch vor der Verschlüsselung, „an der Quelle“, abgehört werden könne. Dies erfordere einen Eingriff in die technischen Prozesse des Endgerätes, das im Rechtssinne ein sogenanntes informationstechnisches System (IT-System) darstelle,

Abgh-Drs. 19/2553, S. 195.

Durch § 26b werde der Polizei gestattet, das informationstechnische System, beispielsweise einen Server, einen PC, einen Laptop, aber auch ein Smartphone, nach bestimmten Kriterien zu durchsuchen,

Abgh-Drs. 19/2553, S. 198.

2. Funktionsweise und Anwendungsszenarien

§ 26a ASOG ermächtigt die Polizei, eine Quellen-Telekommunikationsüberwachung zur Überwachung von verschlüsselter laufender Kommunikation durchzuführen. Heutzutage nutzen viele Kommunikationsprogramme standardmäßig eine Verschlüsselung der Daten, die ohne aktives Handeln der Nutzenden im Hintergrund arbeitet. Zur Umgehung dieser Schutzvorkehrungen erfasst diese besondere Form der Telekommunikationsüberwachung die Kommunikation bereits „an der Quelle“, somit entweder bevor die Daten verschlüsselt oder nachdem diese entschlüsselt wurden. Dazu bedarf es der Infiltration des informationstechnischen Systems mit einer speziellen Software, welche die verdeckte Überwachung möglich macht – dem sogenannten Staatstrojaner. Da die Entwicklung einer solchen Software sehr aufwendig ist, setzen Sicherheitsbehörden oft Lösungen von privaten Dritten ein. Medienberichten zufolge hat etwa das Bundeskriminalamt die Software Pegasus der israelischen NSO Group erworben,

spiegel.de vom 7. September 2021, BKA hat umstrittene Überwachungssoftware von NSO gekauft, <https://www.spiegel.de/netzwelt/netzpolitik/bka-hat-umstrittene-ueberwachungssoftware-von-nso-gekauft-a-8c8039a4-a8d5-49a3-8a4b-afdf98fd165a>.

Auch § 26b ASOG ermächtigt zum Eingriff in informationstechnische Systeme mittels eines Staatstrojaners. Dabei wird jedoch nicht nur auf Kommunikationsdaten zugegriffen, sondern auf alle auf dem informationstechnischen System gespeicherten Daten.

Die für die Durchführung beider Überwachungsbefugnisse notwendige Infiltration der Zielsysteme erfolgt in der Regel, indem die Polizei Schwachstellen in informationstechnischen Systemen ausnutzt.

§ 2 Nr. 38 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) definiert Schwachstelle als „eine Eigenschaft von IKT-Produkten oder IKT-Diensten, die von Dritten ausgenutzt werden kann, um sich gegen den Willen des Berechtigten Zugang zu den IKT-Produkten oder IKT-Diensten zu verschaffen oder die Funktion der IKT-Produkte oder IKT-Dienste zu beeinflussen.“ Bei einem IKT-Produkt kann es sich etwa um ein Smartphone oder eine Software handeln.

Innerhalb dieser Definition werden Schwachstellen danach unterschieden, ob sie den Herstellern bereits bekannt – dann n-Days, im Sinne von: Herstellern bereits seit n Tagen bekannt – oder noch unbekannt sind – dann Zero-Days, Herstellern null Tage bekannt.

Aus der Perspektive der Sicherheit von informationstechnischen Systemen, die mit der fehlerhaften Software arbeiten, unterscheiden sich n-Days und Zero-Days fundamental:

Für Zero-Days stehen noch keine technischen Lösungen – sogenannte Fixes oder Patches – bereit. Eine Ausnahme besteht nur in dem seltenen Fall, dass Hersteller die Software auch in Unkenntnis der Sicherheitslücke durch Zufall so ändern, dass die Lücke gleichsam „nebenbei“ geschlossen wird.

Für n-Days hingegen besteht für die Hersteller des betroffenen Systems die Möglichkeit, Gegenmittel zu entwickeln. Zero-Day-Schwachstellen bergen folglich eine höhere Gefahr. Gerade der Mangel an technischen Lösungen für diese gefährlichen Schwachstellen veranlasst jedoch die Sicherheitsbehörden, diese zu suchen. Dieser Mangel ermöglicht

insbesondere eine längerfristige Ausnutzung der Schwachstellen für die bezweckten Überwachungsmaßnahmen.

Die Gefährlichkeit von Zero-Day-Schwachstellen intensiviert sich zusätzlich, wenn für anfällige Systeme ein funktionierender Angriffscod bereits in bekannte Angriffswerkzeuge integriert wurde. Dies macht eine breitere Ausnutzung – und somit auch einen Missbrauch durch kriminelle Dritte – höchstwahrscheinlich. Das gilt insbesondere für den – gesetzlich nicht ausgeschlossenen und in der Praxis relevanten – Fall, dass die Behörden Angriffswerkzeuge nutzen, die von privaten Unternehmen entwickelt wurden und auch Dritten angeboten werden.

Die §§ 26a, 26b ASOG setzen Anreize für den Ankauf und das Zurückhalten von Zero-Day-Schwachstellen, ohne zu regeln, ob und unter welchen Voraussetzungen die mit den Schwachstellen verbundenen Risiken so hoch sind, dass eine Meldung an den Hersteller geboten ist.

3. Eingriffe in Schutzbereiche

Sowohl die Quellen-Telekommunikationsüberwachung als auch die Online-Durchsuchung greifen in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (IT-Grundrecht oder IT-System-Grundrecht) aus Art. 7 i.V.m. Art. 6 VvB oder Art. 33 VvB ein.

Das Bundesverfassungsgericht hat aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG ein solches Grundrecht abgeleitet,

BVerfGE 120, 274 <302 ff. Rn. 166 ff.>.

Diese Rechtsprechung hat es jüngst bekräftigt und die Schutzrichtung konkretisiert:

„aa) Das IT-System-Grundrecht schützt insbesondere vor heimlichen Zugriffen durch eine Online-Durchsuchung, ist hierauf aber nicht beschränkt.

(1) Schutzgegenstand sind IT-Systeme, die aufgrund ihrer technischen Funktionalität allein oder durch ihre technische Vernetzung Daten einer betroffenen Person in einem Umfang und einer Vielfalt vorhalten können, dass ein Zugriff auf das System es

ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten (vgl. BVerfGE 120, 274 <313 f.>). Dabei kommt es neben der Datenmenge und -vielfalt auch auf deren Qualität an. Denn auch ein vergleichsweise geringer Datenbestand auf einem modernen IT-System kann tiefgreifende Einblicke in die Lebensgestaltung oder die Persönlichkeit einer Person liefern. Insofern stehen Qualität und Quantität von Daten in einem wechselseitigen Verhältnis zueinander: Bei qualitativ hochwertigen und damit aussagekräftigen Daten können bereits wenige Daten einen umfassenden Einblick in die Lebensgestaltung oder Persönlichkeit ermöglichen (vgl. auch BVerfGE 165, 363 <401 Rn. 78>; BVerfG, Beschluss des Ersten Senats vom 14. November 2024 - 1 BvL 3/22 -, Rn. 93).

(2) Grundrechtlich gewährleistet ist die Vertraulichkeit und Integrität des vom Schutzbereich erfassten IT-Systems. Quantität und Qualität der von einem IT-System nach seiner technischen Konstruktion potentiell abschöpfbaren Daten führen zu einer besonderen persönlichkeitsrechtlichen Gefährdungslage bei einem Zugriff. Schutzobjekt ist insoweit aber schon das IT-System selbst. Wird dieses als eigenes genutzt, besteht eine darauf bezogene grundrechtlich anzuerkennende Vertraulichkeits- und Integritätserwartung (näher BVerfGE 120, 274 <315>).

Geschützt ist zunächst das Interesse der Nutzenden, dass die von einem vom Schutzbereich erfassten IT-System erzeugten, verarbeiteten und gespeicherten oder von dort aus zugänglichen Daten (vgl. insoweit BVerfGE 141, 220 <303 f. Rn. 209 f.>) vertraulich bleiben (vgl. BVerfGE 120, 274 <314>). Vom Gewährleistungsgehalt umfasst ist aber auch die Integrität des IT-Systems, die betroffen ist, wenn auf das IT-System so zugegriffen wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können; dann ist die entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems genommen (vgl. BVerfGE 120, 274 <314>).

Das IT-System-Grundrecht schützt mithin nicht nur die Vertraulichkeit der Daten, die durch Datenerhebungsvorgänge verletzt wird, sondern verlagert diesen Schutz nach vorne und umfasst schon die abstrakt-systembezogene Vertraulichkeitserwartung im Vorfeld konkreter Datenerhebungen. Denn bereits mit dem Zugriff auf ein IT-System entsteht – unabhängig davon, welcher Aufwand dafür nötig ist (vgl. BVerfGE 120, 274 <315>) – eine besondere Gefährdungslage für die dort erzeugten, verarbeiteten und gespeicherten oder von dort aus zugänglichen Daten (vgl. auch BVerfGE 120, 274 <308, 314>). Der Gewährleistungsgehalt des IT-System-Grundrechts geht dementsprechend über den Schutz personenbezogener Daten

hinaus und vermittelt einen insoweit vorgelagerten Schutz der Persönlichkeit. Der Schutzbereich ist daher stets vom IT-System her zu definieren und auf ein auf dieses System insgesamt bezogenes Gefährdungspotenzial ausgelegt (vgl. BVerfGE 120, 274 <308 f., 313 ff.>; vgl. auch Hoffmann-Riem, JZ 2008, S. 1009 <1015, 1017>; Lepsius, in: Roggan, Online-Durchsuchungen, 2008, S. 21 <32 ff.>; Bäcker, in: Rensen/Brink, Leitlinien der Rechtsprechung des Bundesverfassungsgerichts, Band 1, 2009, S. 99 <123, 126>; Gersdorf, in: Gersdorf/Paal, BeckOK Informations- und Medienrecht, GG Art. 2 Rn. 28 <November 2024>). Der systembezogene Schutz ist folglich bereits dann berührt, wenn sich Unberechtigte Zugriff auf das IT-System verschaffen und dadurch potenziell Daten abgreifen können – ohne dass dies auch tatsächlich geschehen muss (vgl. Hoffmann/Luch/Schulz/Borchers, Die digitale Dimension der Grundrechte, 2015, S. 70 f., 73; Ruppert, in: Dietrich/Fahrner/Gazeas/von Heintschel-Heinegg, Handbuch Sicherheits- und Staatsschutzrecht, 2022, § 23 Rn. 14).

Als konsequenter Ausdruck seiner systemischen Schutzrichtung schützt das IT-System-Grundrecht das IT-System als virtuellen Raum der Bewahrung und Entfaltung der eigenen Persönlichkeit in seiner ganzen Breite (vgl. auch BVerfGE 158, 170 <184 Rn. 29>; 162, 1 <139 f. Rn. 308>).“

BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025 – 1 BvR 2466/19 –, Rn. 96 ff.

Daran anknüpfend hat das Bundesverfassungsgericht entschieden, dass auch die Quellen-Telekommunikationsüberwachung in das IT-Grundrecht eingreift und dass – insofern wohl abweichend von vorheriger Rechtsprechung – das IT-Grundrecht in diesem Fall nicht hinter das Fernmeldegeheimnis aus Art. 10 Abs. 1 GG zurücktritt,

BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025 – 1 BvR 2466/19 –, Rn. 103 ff., 105 ff.

Der Verfassungsgerichtshof Berlin hat sich – soweit ersichtlich – noch nicht mit der Frage befasst, ob aus den Grundrechten der Verfassung von Berlin ein IT-Grundrecht abzuleiten ist. Art. 6 und Art. 7 VvB entsprechen jedoch Art. 1 Abs. 1 und Art. 2 Abs. 1 GG, sodass es naheliegt, aus diesen Normen ein IT-Grundrecht als Ausprägung des allgemeinen Persönlichkeitsrechts,

vgl. dazu Verfassungsgerichtshof des Landes Berlin, Beschluss vom 24. Januar 2003 – 39/99 –, Rn. 14; Beschluss vom 16. November 2010 – 115/10 –, Rn. 15,

abzuleiten.

Alternativ kann ein solches Grundrecht auch aus Art. 33 VvB abgeleitet werden. Allerdings käme darin die systemische Schutzrichtung des IT-Grundrechts weniger stark zum Ausdruck.

Sowohl die Quellen-Telekommunikationsüberwachung nach § 26a ASOG als auch die Online-Durchsuchung nach § 26b ASOG greifen daneben auch in das Fernmeldegeheimnis aus Art. 16 VvB ein,

vgl. BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025 – 1 BvR 2466/19 –, Rn. 86 ff; Beschluss des Ersten Senats vom 24. Juni 2025 – 1 BvR 180/23 –, Rn. 243.

4. Keine Rechtfertigung

Die Eingriffe sind nicht gerechtfertigt. Sie wiegen schwer (a)), ohne dass sie an hinreichend gehaltvolle Voraussetzungen und Schutzvorkehrungen geknüpft sind (b)).

a) Eingriffsintensität

Die Eingriffe durch die Quellen-Telekommunikationsüberwachung und die Online-Durchsuchung wiegen schwer.

Das Eingriffsgewicht der Quellen-Telekommunikationsüberwachung ist insbesondere höher als bei der „normalen Telekommunikationsüberwachung“, wie das Bundesverfassungsgericht jüngst betont 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 berechnete 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>).“

BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025 – 1 BvR 180/23 –, Rn. 188 ff.

Die Online-Durchsuchung gehört neben der Wohnraumüberwachung zu den schwerwiegendsten Grundrechtseingriffen,

vgl. BVerfGE 120, 274 <322 ff. Rn. 229 ff.>.

Da auf sämtliche gespeicherte Daten zugegriffen werden kann, ist das Eingriffsgewicht gegenüber der Quellen-Telekommunikationsüberwachung gesteigert,

vgl. BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025 – 1 BvR 180/23 –, Rn. 242.

b) Unzureichende Eingriffsvoraussetzungen

Die Eingriffsvoraussetzungen genügen nicht den grundrechtlichen Anforderungen.

Verfassungsrechtliche Anforderungen richten sich dabei sowohl an die sogenannte Eingriffsschwelle, also den Anlass der Überwachung, als auch an das mit der Datenerhebung zu schützende Rechtsgut. Erforderlich als Anlass ist bezogen auf die Gefahrenabwehr grundsätzlich eine im Einzelfall vorliegende konkrete Gefahr im Sinne der polizeirechtlichen Generalklauseln oder eine wenigstens konkretisierte Gefahr. Eine Absenkung der Eingriffsschwelle auf die konkretisierte Gefahr ist aus Gründen der Verhältnismäßigkeit regelmäßig mit erhöhten Anforderungen an die konkret geschützten Rechtsgüter verbunden. Zu berücksichtigen ist stets auch das Eingriffsgewicht der konkreten Maßnahme. Je tiefer

Überwachungsmaßnahmen in das Privatleben hineinreichen und berechnete Vertraulichkeitserwartungen überwinden, desto strenger sind die Anforderungen an ihre Rechtfertigung. Die Erhebung von Daten durch Überwachungsmaßnahmen mit hoher Eingriffsintensität ist daher im Bereich der Gefahrenabwehr grundsätzlich nur dann verhältnismäßig, wenn eine Gefährdung besonders gewichtiger Rechtsgüter im Einzelfall hinreichend konkret absehbar ist und der Adressat der Maßnahmen aus Sicht eines verständigen Dritten den objektiven Umständen nach in sie verfangen ist,

BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025 – 1 BvR 2466/19 –, Rn. 126.

§§ 26a, 26b ASOG genügen teilweise weder mit Blick auf die Rechtsgüter (aa)) noch mit Blick auf die Eingriffsschwelle (bb)) den verfassungsrechtlichen Anforderungen. Zudem enthalten die Befugnisse eine unzulässige dynamische Verweisung auf Bundesrecht (cc)).

aa) Rechtsgüterschutz

Heimliche Überwachungsmaßnahmen, die – wie hier – tief in das Privatleben hineinreichen, sind nur zum Schutz besonders gewichtiger Rechtsgüter zulässig, zu denen vor allem Leib, Leben und Freiheit der Person sowie Bestand oder Sicherheit des Bundes oder eines Landes zählen,

BVerfGE 165, 363 <410 Rn. 105>; 141, 220 <270 f. Rn. 108>.

Der uneingeschränkte Schutz von Sachwerten ist dem gegenüber nicht ausreichend,

BVerfGE 141, 220 <270 f. Rn. 108>.

Als hinreichend gewichtige Rechtsgüter kommen daher nicht schon Sachwerte mit bedeutendem Wert in Betracht, sondern „im gesetzlichen Zusammenhang mit der Terrorismusabwehr vielmehr etwa wesentliche Infrastruktureinrichtungen oder sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen [...]“,

BVerfGE 141, 220 <287 f. Rn. 155>; 165, 363 <410 Rn. 105>.

Der Gesetzgeber muss die Rechtsgüter nicht unmittelbar benennen, sondern kann auch an entsprechende Straftaten anknüpfen, deren Verhütung er mit der Befugnis bezweckt,

BVerfGE 165, 363 <410 Rn. 105 a.E.>.

Benennt er das zu schützende Rechtsgut nicht unmittelbar, sondern knüpft an Straftatbestände an, müssen diese entsprechend schwer wiegen. 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, unter bestimmten Voraussetzungen auch solche mit einer Höchstfreiheitsstrafe von fünf Jahren,

BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025 – 1 BvR 2466/19 –, Rn. 137.

Aber auch dann ist zu fordern, dass der jeweilige Tatbestand ein besonders gewichtiges Rechtsgut schützt. Ansonsten käme es zu einer inkohärenten Aufspaltung der verfassungsrechtlichen Anforderungen an präventivpolizeiliche Überwachungsermächtigungen. Dies eröffnete dem Gesetzgeber die Möglichkeit, die strengen Anforderungen an das zu schützende Rechtsgut zu umgehen, indem er den Eingriffstatbestand durch Bezugnahme auf Straftaten gestaltet.

Zugleich steht dem Gesetzgeber die Entscheidung über den gesetzlichen Strafraum weitgehend frei. So könnte der Gesetzgeber weitreichende Überwachungsermächtigungen ermöglichen, indem er schlicht die gesetzlichen Strafraum einschlägiger Delikte weitgehend ohne Rücksicht auf deren Schutzgüter erhöht.

Es ist daher zu fordern, dass eine Straftat nur dann als Anknüpfungspunkt für eine tief in die Grundrechte eingreifende heimliche Ermittlungsmaßnahme herangezogen werden kann, wenn sie dem Schutz eines besonders gewichtigen Rechtsguts dient,

BVerwG, Beschluss vom 31. Mai 2022 – 6 C 2.20 –, Rn. 33.

Dies entspricht auch den Anforderungen, die das Bundesverfassungsgericht im Rahmen seiner befristeten Anordnung

der Fortgeltung der verfassungswidrigen hessischen Ermächtigungsgrundlagen für die automatisierte Datenanalyse 2023 an den Verweis auf § 100b Abs. 2 StPO stellte,

vgl. BVerfGE 165, 363 <440 Rn. 176>.

§ 26a Abs. 1 Nr. 1 lit b) ASOG knüpft mit seinem Verweis auf § 100b Abs. 2 StPO nicht an die Gefährdung besonders gewichtiger Rechtsgüter an. Dieser Mangel betrifft auch § 26a Abs. 1 Nr. 3 und § 26b Abs. 1 und 2 ASOG, soweit diese Normen auf § 26a Abs. 1 Nr. 1 lit. b) ASOG verweisen.

Die im Katalog des § 100b Abs. 2 StPO genannten Straftatbestände dienen zwar teilweise auch dem Schutz besonders gewichtiger Rechtsgüter. Jedoch gilt das nicht für alle dort genannten Tatbestände.

Insbesondere knüpft § 100b Abs. 2 StPO in seinem Katalog auch an eine Vielzahl von Delikten an, die primär Vermögen oder Eigentum schützen, obwohl bedeutsame Sachwerte nur in den durch das Bundesverfassungsgericht definierten engen Grenzen („wesentliche Infrastruktureinrichtungen oder sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen [...]“) ein zulässiges Schutzgut darstellen,

BVerfGE 165, 363 <410 Rn. 105>; 141, 220 <287 f. Rn. 155>.

Damit sind insbesondere die folgenden Delikte nicht als besonders schwere Straftaten anzusehen:

- § 100b Abs. 2 Nr. 1 lit. d) StPO (Geld- und Wertzeichenfälschungen)
- § 100b Abs. 2 Nr. 1 lit. i) StPO (Bandendiebstahl)
- § 100b Abs. 2 Nr. 1 lit. j) StPO (jedenfalls hinsichtlich des schweren Raubes, § 250 Abs. 1, 2 StGB, soweit es nicht Tateinheitlich zu Körperverletzungen kam)
- § 100b Abs. 2 Nr. 1 lit. k) StPO (räuberische Erpressung und besonders schwerer Fall der Erpressung, soweit es nicht Tateinheitlich zu Körperverletzungen kam)
- § 100b Abs. 2 Nr. 1 lit. l) StPO (Qualifikationen der Hehlerei)
- § 100b Abs. 2 Nr. 1 lit. m) StPO (Geldwäsche)

- § 100b Abs. 2 Nr. 1 lit. n) StPO (Computerbetrug)
- § 100b Abs. 2 Nr. 1 lit. b) StPO (Betrieb krimineller Handelsplattformen, sofern sich lit. b) auf die zuvor genannten Ziffern und Straftaten bezieht).

Ebenso wenig genügen Verstöße gegen das Asyl- oder Aufenthaltsgesetz, sodass § 100b Abs. 2 Nr. 2 und 3 StPO keine besonders schweren Straftaten beinhalten.

Eine andere Beurteilung der Straftaten in § 100b Abs. 2 StPO hinsichtlich der geschützten Rechtsgüter folgt auch hier nicht daraus, dass das Bundesverfassungsgericht im Rahmen seiner befristeten Anordnung der Fortgeltung der verfassungswidrigen hessischen Ermächtigungsgrundlage im Datenanalyseurteil ebenfalls auf § 100b Abs. 2 StPO verwies,

BVerfGE 165, 363 <440 Rn. 176>.

Dem kann gerade nicht entnommen werden, dass allein ein Verweis auf den Katalog des § 100b Abs. 2 StPO durch den Gesetzgeber zum dauerhaften Schutz der Grundrechte genügen würde und dass der Katalog zum Schutz besonders wichtiger Rechtsgüter genügt, da das Bundesverfassungsgericht die Gefährdung besonders gewichtiger Rechtsgüter ausdrücklich neben der Gefahr einer Straftat nach § 100b Abs. 2 StPO gefordert hat.

Das Bundesverfassungsgericht hat vielmehr zuletzt in einer Entscheidung mangels Entscheidungserheblichkeit offengelassen, ob § 100b Abs. 2 StPO hinreichend gewichtige Rechtsgüter und Schwellen vorsieht,

BVerfGE 162, 1 <172 Rn. 388>.

Selbst wenn das angerufene Gericht davon ausginge, der Gesetzgeber könne an besonders schwere Straftaten anknüpfen, ohne eine ergänzende Rechtsgutsbetrachtung vorzunehmen, würde der Verweis auf § 100b Abs. 2 StPO diesen Anforderungen nicht genügen.

Der Strafraum hat zwar eine Indizwirkung für die Beurteilung der besonderen Schwere einer Straftat. Eine Straftat mit einer angedrohten

Höchstfreiheitsstrafe von fünf Jahren kann aber auch dann 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“,

BVerfGE 169, 130 <219 Rn. 205>.

Die Qualifizierung als besonders schwere Straftat muss in der Strafnorm selbst einen objektivierten Ausdruck finden, insbesondere im Strafraumen und ggf. in tatbestandlich umschriebenen oder in einem Qualifikationstatbestand enthaltenen Begehungsmerkmalen und Tatfolgen,

BVerfGE 169, 130 <220 Rn. 206>.

Für Wohnraumüberwachungen, Online-Durchsuchungen und Quellen-Telekommunikationsüberwachungen hat das Bundesverfassungsgericht einen Strafraumen mit Höchstfreiheitsstrafe von mindestens fünf Jahren nicht ausreichen lassen,

BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025 – 1 BvR 180/23 –, Rn. 210; BVerfGE 169, 130 <219 Rn. 205>; 141, 220 <338 Rn. 316>.

Jedenfalls keine besonders schweren Straftaten in diesem Sinne sind Delikte, die lediglich einen Strafraumen von bis zu drei Jahren Freiheitsstrafe oder Geldstrafe vorsehen,

BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025 – 1 BvR 180/23 –, Rn. 211; BVerfGE 169, 130 <219 Rn. 205>; 163, 43 <102 Rn. 155>; 165, 1 <93 Rn. 180>.

Auch unter Anwendung dieses Maßstabs genügt § 100b Abs. 2 StPO den verfassungsrechtlichen Anforderungen nicht.

Dies ergibt sich zum einen daraus, dass § 100b StPO umfänglich, teils ausdrücklich, auf minder schwere Fälle verweist, deren Einstufung als besonders schwere Straftaten weder ihrem Strafmaß nach indiziert ist noch im Tatbestand der Norm einen den Vorgaben entsprechenden objektivierten Ausdruck findet. Minder schwere Fälle, die im Höchstmaß mit Freiheitsstrafe von fünf Jahren bestraft sind, finden sich in den § 82

Abs. 2 StGB, § 89a Abs. 5 StGB, § 100 Abs. 3 StGB, § 146 Abs. 3 StGB, § 152b Abs. 3 StGB, § 234 Abs. 2 StGB, § 234a Abs. 2 StGB (explizite gesetzliche Inbezugnahme), § 244a Abs. 2 StGB, § 260a Abs. 2 StGB, § 263 Abs. 5 StGB, § 84a Abs. 2 AsylG und § 29a Abs. 2 BtMG.

Dass der Gesetzgeber bewusst auch die Begehungsfahr dieser minder schweren Fälle als Eingriffsschwelle ausreichen lassen wollte, ergibt sich nicht zuletzt daraus, dass in einigen Verweisungsnormen Bezugnahmen auf diejenigen Absätze, die einen minder schweren Fall regeln, dezidiert ausgespart wurden, etwa § 89c Abs. 5 StGB, § 233a Abs. 4 Halbsatz 1 StGB oder § 30 Abs. 2 BtMG. Im Übrigen wird bezüglich vieler anderer Straftaten von vornherein auf besonders schwere Fälle verwiesen, etwa in den § 95 Abs. 3 StGB, § 98 Abs. 1 Satz 2 StGB oder § 99 Abs. 2 StGB.

Erreichen diese minder schweren Fälle aber nicht den verfassungsrechtlich vorgegebenen Höchststrafrahmen, erscheint ihre Einstufung als besonders schwere Straftaten in fast allen Fällen auch unter Berücksichtigung der jeweils geschützten Rechtsgüter und deren Bedeutung für die Rechtsgemeinschaft sowie der erfassten Tatbegehung und der Tatfolgen nicht vertretbar.

Hier seien dafür nur einige Beispiele herausgegriffen: Über § 100b Abs. 2 Nr. 1 lit. d) StPO ist beispielsweise auf die Geld- oder Wertpapierfälschung in einem minder schweren Fall gemäß § 146 Abs. 3 StGB bzw. § 151 StGB verwiesen. Nach der eigenen Wertung des Gesetzgebers kann für eine solche Tatbegehung schon eine Strafe von drei Monaten Freiheitsstrafe ausreichen. Eine besonders schwere Art der Tatbegehung oder besonders schwere Tatfolgen sind nicht ersichtlich, finden aber jedenfalls in der Strafnorm selbst keinen objektivierenden Ausdruck. Konkret würde also beispielsweise schon die konkretisierte Gefahr der Herstellung geringfügigster Mengen von Falschgeld, beispielsweise auch nur eines einzelnen Scheins, ausreichen.

Ähnliche Ungleichgewichte können beim Verdacht der gewerbsmäßigen Bandenhehlerei gemäß § 260a StGB entstehen, die im minder schweren Fall gemäß § 260a Abs. 2 StGB mit einer Freiheitsstrafe von sechs Monaten bis fünf Jahren bestraft wird. Auch

hier zeigt die Aufnahme eines minder schweren Falles an, dass der Gesetzgeber selbst nicht davon ausgeht, dass es sich notwendigerweise um eine besonders schwere Straftat handelt.

Zuletzt genannt sei auch noch § 29a BtMG, im minder schweren Fall gemäß Abs. 2 wiederum mit einer Mindestfreiheitsstrafe von drei Monaten bestraft. Erfasst ist danach auch schon der Besitz von Betäubungsmitteln in nicht geringer Menge in einem minder schweren Fall.

bb) Eingriffsschwelle

Die verfassungsrechtliche Rechtfertigung eines Eingriffs in informationstechnische Systeme, um aus ihnen Daten zu erheben, setzt eine konkretisierte Gefahr einer Rechtsgutsverletzung voraus,

BVerfG, Beschluss des Ersten Senats vom 9. Dezember 2022 – 1 BvR 1345/21 –, Rn. 128.

Auch die (Quellen-)Telekommunikationsüberwachung setzt mindestens eine konkretisierte Gefahr voraus,

BVerfG, Beschluss des Ersten Senats vom 9. Dezember 2022 – 1 BvR 1345/21 –, Rn. 160.

Danach sind Maßnahmen gegen eine Person zulässig, wenn entweder Tatsachen die Annahme rechtfertigen, dass diese Person innerhalb eines überschaubaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine terroristische Straftat begehen wird, oder das individuelle Verhalten dieser Person die konkrete Wahrscheinlichkeit dafür begründet, dass sie innerhalb eines überschaubaren Zeitraums eine terroristische Straftat begehen oder an dieser teilnehmen wird,

BVerfG, Beschluss des Ersten Senats vom 9. Dezember 2022 – 1 BvR 1345/21 –, Rn. 95.

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,

BVerfG, Beschluss des Ersten Senats vom 9. Dezember 2022 – 1 BvR 1345/21 –, Rn. 95; Urteil des Ersten Senats vom 16. Februar 2023 – 1 BvR 1547/19 –, Rn. 170.

Der Gesetzgeber hat versucht, diese Vorgaben in § 17 Abs. 6 ASOG umzusetzen. Das ist ihm jedoch nicht gelungen.

Nach dieser Norm wird bei Bezugnahmen auf bestimmte Vorfelddelikte vorausgesetzt, dass „zudem eine solche konkretisierte Gefahr für das durch den jeweiligen Straftatbestand geschützte Rechtsgut“ besteht. Dieses „durch den jeweiligen Straftatbestand geschützte Rechtsgut“ ist jedoch nicht immer einfach zu bestimmen. So soll das Schutzgut von § 129a StGB die „öffentliche Sicherheit“, der „öffentliche Friede“, oder die „innere Sicherheit“ sein,

vgl. Eschelbach, in: NK-StGB, 6. Aufl. 2023, § 129a Rn. 14.

Hierbei ist bereits fraglich, ob es sich überhaupt um Rechtsgüter im Sinne der Rechtsprechung des Bundesverfassungsgerichts handelt. Jedenfalls handelt es sich wegen deren Weite nicht stets um besonders gewichtige Rechtsgüter. Folgt man indes der Auffassung, dass auf die Bezugsstraftaten des § 129a StGB abzustellen ist, sind die Rechtsgüter einfacher zu bestimmen. Jedoch stellt sich dann die Frage, wozu es einer Bezugnahme auf das Vorfelddelikt überhaupt bedarf.

Es ist mithin nicht hinreichend bestimmt und normenklar geregelt, dass eine konkretisierte Gefahr für ein besonders gewichtiges Rechtsgut bestehen muss,

kritisch auch Bäcker, Stellungnahme zu dem Entwurf eines Gesetzes zur Änderung polizeirechtlicher Vorschriften (LT-Drs. 8/6142), **Anlage 11**, S. 7 f.

Für die Verfassungsmäßigkeit spricht auch nicht, dass die Formulierung in § 17 Abs. 6 ASOG fast wortgleich den genannten Entscheidungen des Bundesverfassungsgerichts entnommen ist. Das Bundesverfassungsgericht ist nicht der Gesetzgeber und muss mithin nicht dem Grundsatz der Bestimmtheit und Normenklarheit genügen.

Der parlamentarische Gesetzgeber muss hingegen dieser Verantwortung gerecht werden und darf sich nicht damit begnügen, verfassungsgerichtliche Rechtsprechung partiell abzuschreiben.

cc) Unzulässiger dynamischer Verweis

Zudem ist die dynamische Verweisung auf § 100b Abs. 2 StPO in § 26a Abs. 1 Nr. 1 lit b) ASOG schon ihrer Form nach nicht mit verfassungsrechtlichen Anforderungen an Bestimmtheit und Normenklarheit vereinbar,

vgl. BVerfGE 162, 1 (169 Rn. 383 ff.) ebenfalls zu einer Verweisung auf § 100b Abs. 2 StPO in einer sicherheitsrechtlichen Ermächtigungsgrundlage (Art. 8b Abs. 2 BayVSG a.F.).

Der Landesgesetzgeber muss nicht alle Einzelheiten des gesetzlichen Tatbestandes selbst festlegen, sondern kann auf andere Regelungen auch eines anderen Normgebers verweisen,

BVerfGE 162, 1 (169 Rn. 384); 153, 310 (343 f. Rn. 79); 143, 38 (55); 141, 143 (176 f.); 29, 198 (210); 26, 338 (366 f.).

Dabei ist zwischen statischen und dynamischen Verweisungen zu unterscheiden.

Statische Verweisungen auf die Fassung eines Gesetzes, wie sie bei Erlass des Gesetzesbeschlusses galt, sind zulässig,

vgl. BVerfGE 162, 1 <169 Rn. 384> m.w.N.; 153, 310 <343 f. Rn. 79>; 143, 38 <57>; 41, 143 <176 f.>.

Strengere Anforderungen gelten jedoch für dynamische Verweisungen. Diese sind nur im Rahmen von Rechtsstaats- und Demokratieprinzip, mithin insbesondere im Rahmen grundrechtlicher Gesetzesvorbehalte zulässig. Ermächtigen Gesetze zu einem Eingriff in Grundrechte, muss der Gesetzgeber die erforderliche Abwägung des betroffenen Grundrechts mit entgegenstehenden Grundrechten, anderen Verfassungsbelangen und sonstigen schützenswerten Interessen selbst vornehmen. Es muss gewährleistet sein, dass der Gesetzgeber die Abwägungsentscheidung in voller Verantwortung trifft,

BVerfGE 162, 1 <169 f. Rn. 385>; 143, 38 <57>; 141, 143 <176 f.>.

Dies ist bei dynamischen Verweisungen von Landesgesetzen auf bundesgesetzliche Regelungen nicht ohne Weiteres gewährleistet, da der Bundesgesetzgeber nicht verpflichtet ist, in seine Abwägungsentscheidungen Rückwirkung seiner Norm auf landesgesetzgeberische Abwägungsentscheidungen zu berücksichtigen. Aufgrund der Dynamik der Verweisung kann der Landesgesetzgeber nicht abwägen, was er nicht vollständig überblickt. Daher sind dynamische Verweisungen des Landesgesetzes auf bundesgesetzliche Normen nur ausnahmsweise dann möglich, wenn die in Bezug genommenen Regelungen ein eng umrissenes Feld betreffen und deren Inhalt im Wesentlichen bereits feststeht,

BVerfGE 162, 1 <169 f. Rn. 385> m.w.N.

§ 26a Abs. 1 Nr. 1 lit b) ASOG enthält eine solche dynamische Verweisung. Weder dem Wortlaut noch der Gesetzesbegründung ist zu entnehmen, dass auf § 100b Abs. 2 StPO in der Fassung zum Zeitpunkt des Gesetzesbeschlusses verwiesen werden soll. Vielmehr wird § 100b Abs. 2 StPO pauschal in Bezug genommen,

Abgh-Drs. 19/2553, S. 196.

Die dynamische Verweisung ist auch nicht ausnahmsweise zulässig, weil § 100b Abs. 2 StPO gerade kein eng umrissenes Feld regelt, dessen Inhalt weitgehend feststünde. Da das Sicherheitsrecht ein Feld intensiver politischer Auseinandersetzung ist, sind weitere Änderungen des Katalogs in § 100b Abs. 2 StPO schwer abzusehen,

BVerfGE 162, 1 <170 Rn. 386> zu einem dynamischen Verweis auf § 100b Abs. 2 StPO in einer sicherheitsrechtlichen Ermächtigungsgrundlage.

c) Fehlende Überprüfung der genutzten Software

§§ 26a, 26b ASOG genügen zudem nicht dem Verhältnismäßigkeitsgrundsatz, weil sie zum Einsatz technischer Mittel ermächtigen, ohne dass diese unabhängig überprüft werden.

Eine nähere Beschreibung der eingesetzten „technischen Mittel“ findet sich weder im Gesetz noch in der Begründung.

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

Diese technischen Anforderungen entsprechen der Rechtsprechung des Bundesverfassungsgerichts,

siehe insbesondere BVerfGE 120, 274 <338 Rn. 281>.

Sie werden jedoch nicht verfahrensrechtlich abgesichert.

Das nach § 26 Abs. 2 ASOG und § 26b Abs. 6 ASOG anordnende Gericht hat zwar die Rechtmäßigkeit der Maßnahme zu überprüfen. Es ist jedoch unklar, ob hierzu auch die Überprüfung der oben genannten Anforderungen gehört. Für eine solche Überprüfung ist das Gericht auch nicht ausgestattet, sodass es sich bestenfalls auf die Angaben der Polizei verlässt. Dies führt im Ergebnis dazu, dass die Polizei beliebige Staatstrojaner einsetzen kann.

Auch die stichprobenartige Kontrolle durch die Berliner Beauftragte für Datenschutz und Informationsfreiheit nach § 51b Satz 1 Nr. 1 ASOG bezieht sich nicht ausdrücklich auf die Anforderungen an die eingesetzte Software.

Ein derart blindes Vertrauen in die von der Polizei einzusetzenden Staatstrojaner ohne einen rechtsstaatlich ausreichenden Überprüfungsmechanismus ist 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 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,

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.

Ob eine modifizierte Version den Anforderungen des deutschen Rechts 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,

BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025 – 1 BvR 2466/19 –, Rn. 114.

Der Gesetzgeber 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. Es bedarf es einer obligatorischen Prüfung beispielsweise durch die Landesbeauftragte für den Datenschutz auf Ebene des Quelltextes, weil nur diese oder eine ähnlich unabhängige Stelle die Gewähr für eine wirklich neutrale Begutachtung der Software bietet. Solange dies nicht vorgesehen ist, trifft die geltende Regelung das Verdikt der Verfassungswidrigkeit.

d) Fehlendes Schwachstellenmanagement

Durch die Ermächtigung zur Ausnutzung von Schwachstellen ohne gleichzeitige Einführung von Schutzvorschriften in Form eines Schwachstellenmanagements entstehen zudem Risiken für die IT-Sicherheit, die mit dem IT-Grundrecht nicht vereinbar sind.

Aus dem IT-Grundrecht folgt eine Schutzpflicht des Staates für die IT-Sicherheit (aa)). Um dieser Schutzpflicht zu genügen, ist ein Schwachstellenmanagement erforderlich, das zumindest in Grundzügen gesetzlich geregelt sein muss (bb)). Weder das ASOG noch andere Normen sehen ein solches Schwachstellenmanagement vor (cc)).

aa) Schutzpflicht für die IT-Sicherheit

Das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme umfasst auch die objektive Schutzpflicht des Staates, zum Schutz informationstechnischer Systeme vor Angriffen durch Dritte beizutragen. Die staatliche Schutzpflicht 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,

vgl. BVerfGE 158, 170 <189 f. Rn. 44>.

Damit wird der staatliche Schutzauftrag explizit an den beschriebenen Zielkonflikt geknüpft und der großen Bedeutung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme für die Funktionsfähigkeit und die Sicherheit von Staat und Gesellschaft Rechnung getragen. Somit werden die hohen, gegenwärtigen Gefahren berücksichtigt, welche die Schwachstellen in IT-Systemen für gewichtige Rechtsgüter für eine hohe Zahl an potenziell betroffenen Grundrechtsträgern mit sich bringen.

Soweit zudem die dem Fernmeldegeheimnis aus Art. 10 Abs. 1 GG unterfallende Kommunikation ebenfalls durch die Sicherheitslücken bedroht ist, besteht auch insoweit eine staatliche Schutzpflicht.

BVerfGE 158, 170 <185 Rn. 32>.

Die Ausnutzung von Schwachstellen in informationstechnischen Systemen kann gravierende Folgen haben.

Schwachstellen sind in alltäglichen informationstechnischen Systemen keine Ausnahme, sondern der Normalfall. Laut dem BSI ist die informationstechnische Sicherheitslage in Deutschland angespannt bis kritisch. Der Bericht zur Lage der IT-Sicherheit in Deutschland 2025 zeigt, dass die Gefahren im Cyber-Raum weiter zunehmen und auch kritische Bereiche betreffen, wie etwa die Strom- oder die medizinische Versorgung. Nicht nur die Anzahl von Sicherheitsvorfällen ist besorgniserregend, sondern auch die rasante Entwicklung neuer und angepasster Angriffsmethoden, die massenhafte Ausnutzung schwerwiegender Software-Schwachstellen und die teilweise gravierenden Folgen, die erfolgreiche Cyber-Angriffe auslösen,

Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2025, <https://medien.bsi.bund.de/lagebericht/de/index.html>.

Derartige Angriffe können zu erheblichen Gefahren führen, wie viele der Fälle der letzten Jahre immer wieder aufgezeigt haben.

So hat im Mai 2017 das Schadprogramm WannaCry weltweit Schäden verursacht, indem es die informationstechnischen Systeme von Behörden und Unternehmen, insbesondere auch von britischen Krankenhäusern lahmlegte und nur gegen Lösegeldzahlung wieder freigab. Die Sicherheitslücken, welche die hinter WannaCry stehenden Kriminellen ausnutzten, waren zuvor dem amerikanischen Nachrichtendienst NSA gestohlen worden,

vgl. zeit.de vom 15. Mai 2017, Microsoft gibt US-Regierung Mitschuld an Hackerangriff, <https://www.zeit.de/digital/internet/2017-05/wannacry-microsoft-nsa-hackerangriff-usa-regierung>.

Es sind keine Anhaltspunkte dafür ersichtlich, dass deutsche Sicherheitsbehörden Informationen über Zero-Day-Schwachstellen besser schützen könnten als die NSA.

Auch die öffentliche Verwaltung kann zum Ziel von schwerwiegenden Cyberangriffen werden. So wurde jüngst die Berliner Verwaltung durch einen Angriff weitgehend lahmgelegt, bei dem auch sensible Daten abgeflossen sein sollen,

rbb24.de vom 17. August 2026, Hackerangriff auf Berliner Landesnetz verübt - sensible Daten abgeflossen, <https://www.rbb24.de/politik/beitrag/2026/08/berlin-landesnetz-sicherheitsvorfall-it-senatsverwaltung.html>.

Auch das Berliner Kammergericht ist bereits Opfer eines massiven Cyberangriffs geworden,

LTO vom 31. Januar 2020, Keine Entspannung nach Cyberangriff, <https://www.lto.de/recht/justiz/j/kg-berlin-it-sicherheit-cyber-angriff-hacker>.

Solche Angriffe werden eher zu- als abnehmen. Im Zusammenhang mit dem Ukraine-Krieg werden Cyberangriffe von Russland bewusst als Mittel der Kriegsführung gegen die Ukraine, aber auch ihre Verbündeten, eingesetzt,

BSI, Cybersicherheitslage im Zusammenhang mit dem russischen Angriff auf die Ukraine, <https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Threat-Intelligence/Krisen-Grosslagen/Ukraine-Krise/ukraine-krise.html>.

Zahlreiche Vorfälle zeigen auf, dass sich die Gefährdungslage mit Blick auf Cyberattacken weltweit zuspitzt, und zahlreiche und bedeutende Güter von Verfassungsrang regelmäßig betroffen sind. Ein einzelner Cyberangriff geht zumeist mit der Betroffenheit einer großen Zahl an Grundrechtsträger*innen einher. Darüber hinaus beschränken sich die Auswirkungen von Cyberangriffen – wegen der Breite der Nutzung und der Abhängigkeit von Informationstechnik – nicht auf die Vertraulichkeit und Integrität des angegriffenen Systems oder die Offenbarung von

personenbezogenen Daten, sondern haben das Potenzial letztlich sämtliche grundrechtlich geschützten Positionen zu gefährden,

Vgl. BVerfGE 158, 170 <187 Rn. 37>.

bb) Erfordernis eines Schwachstellenmanagements

Um seiner Schutzpflicht für die IT-Sicherheit gerecht zu werden, muss der Gesetzgeber den Umgang mit Schwachstellen regeln.

Grundsätzlich steht dem Gesetzgeber bei der Erfüllung grundrechtlicher Schutzpflichten ein weiter Einschätzungs-, Wertungs- und Gestaltungsspielraum zu. Dieser an der Effektivität des Grundrechtsschutzes ausgerichtete Spielraum kann sich hinsichtlich des Umfangs und Form der Regelung verengen, je nachdem, welcher Sachbereich und welche Rechtsgüter betroffen sind,

vgl. BVerfG, Beschluss vom 16. Dezember 2021 – 1 BvR 1541/20 –, Rn. 99.

Darüber hinaus gebietet es die Wesentlichkeitstheorie, welche sich aus dem grundlegenden Demokratie- und Rechtsstaatsprinzip ableiten lässt, dass der Gesetzgeber es nicht der Exekutive überlassen darf, wesentliche Entscheidungen mit hoher Grundrechtsrelevanz zu treffen, sondern diese selbst im Wege eines Parlamentsgesetzes zu regeln hat.

Vgl. BVerfGE 41, 251 <259 f.>; 45, 400 <417 f.>.

Nach der Rechtsprechung des Bundesverfassungsgerichts gebietet gerade die Schutzpflicht des Rechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme eine Beschränkung des gesetzgeberischen Spielraums. So verlangt die Schutzpflicht eine Regelung darüber, wie eine Behörde bei der Entscheidung über ein Offenhalten unerkannter Sicherheitslücken den Zielkonflikt zwischen dem notwendigen Schutz vor Infiltration durch Dritte einerseits und der Ermöglichung von Quellen-Telekommunikationsüberwachungen andererseits aufzulösen hat. Der Behörde muss eine Abwägung der gegenläufigen Belange für den Fall aufgegeben werden, dass ihr eine Zero-Day-Schutzlücke bekannt wird. Es ist sicherzustellen, dass die Behörde bei jeder Entscheidung über ein Offenhalten einer unbekannten Sicherheitslücke einerseits die Gefahr einer weiteren Verbreitung der Kenntnis von dieser

Sicherheitslücke ermittelt und andererseits den Nutzen möglicher behördlicher Infiltrationen mittels dieser Lücke quantitativ und qualitativ bestimmt, beides zueinander ins Verhältnis setzt und die Sicherheitslücke an Hersteller meldet, wenn nicht das Interesse an der Offenhaltung der Lücke überwiegt,

vgl. BVerfGE 158, 170 <189 f. Rn. 44>.

Unter Berücksichtigung der unüberschaubaren Zahl an betroffenen Personen und besonders bedeutsamen Rechtsgütern ist die Entscheidung über die Ausgestaltung eines Schwachstellenmanagements von so wesentlicher Bedeutung, dass diese einer konkreten parlamentsgesetzlichen Form bedarf. Denn die durch die Schwachstellen entstehenden Gefahren für die Integrität informationstechnischer Systeme und die IT-Sicherheit einer unbestimmten Vielzahl von Grundrechtsträgerinnen sind nicht lediglich faktische Begleiterscheinungen der Maßnahmen, sondern verfassungsrechtlich erhebliche Belastungen,

vgl. BVerfGE 120, 274 <325 f. Rn. 239 ff>; BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025 – 1 BvR 180/23 –, Rn. 193 f.; Wischmeyer/Friedl, Staatlicher Umgang mit IT-Schwachstellen und Spyware, Rechtsgutachten für die Gesellschaft für Freiheitsrechte 2026,

<https://freiheitsrechte.org/uploads/publications/Digital/Rechtsgutachten-Spyware.pdf>, S. 37 ff.

Das Gesetz muss insbesondere ein strukturiertes Verfahren vorsehen, in dem der Nutzen einer Geheimhaltung für die Aufgabenerfüllung der Sicherheitsbehörden gegen die Gefahren für die Informationssicherheit und die betroffenen Grundrechte abgewogen wird. Dabei hat der Gesetzgeber ein Regel-Ausnahme-Verhältnis zugunsten der Offenlegung vorzusehen: Die Meldung einer Schwachstelle an den Hersteller muss den Regelfall bilden, während eine Geheimhaltung nur ausnahmsweise und zeitlich begrenzt zulässig sein darf. Ferner muss das Gesetz die zuständige Entscheidungsinstanz und die Grundzüge des Entscheidungsverfahrens festlegen. Wird eine Schwachstelle ausnahmsweise nicht offengelegt, sind risikomindernde Maßnahmen, eine regelmäßige Überprüfung der Fortdauer der Geheimhaltungsentscheidung sowie wirksame Vorkehrungen zum

Schutz der Schwachstelleninformationen vor Verlust oder unbefugtem Zugriff gesetzlich sicherzustellen. Schließlich bedarf es einer unabhängigen Kontrollinstanz, die über ausreichende Informationen, fachliche Expertise und Ressourcen verfügt, um die Rechtmäßigkeit der Geheimhaltungsentscheidungen wirksam überprüfen zu können,

vgl. Wischmeyer/Friedl, Staatlicher Umgang mit IT-Schwachstellen und Spyware, Rechtsgutachten für die Gesellschaft für Freiheitsrechte 2026, <https://freiheitsrechte.org/uploads/publications/Digital/Rechtsgutachten-Spyware.pdf>, S. 43 ff.

cc) Fehlen eines Schwachstellenmanagements

Ein solches Schwachstellenmanagement ist gesetzlich nicht vorgesehen. Dies führt zur Verfassungswidrigkeit der §§ 26a, 26b ASOG.

Es ergibt sich insbesondere nicht aus § 26a Abs. 2 Satz 2 ASOG, wonach das eingesetzte Mittel nach dem Stand der Technik gegen unbefugte Nutzung zu schützen ist. Als Mittel werden gemeinhin Handlungen oder Gegenstände bezeichnet, die zielgerichtet eingesetzt werden, um einen Zweck zu erreichen. Mittel zeichnen sich dadurch aus, dass die handelnde Person sie in einem Mindestmaß beherrscht und auf den Einsatzzweck zurichtet. Von Mitteln abzugrenzen sind Gegenstände, auf die sich eine zweckgerichtete Handlung bezieht, also die Objekte dieser Handlung. Bei der Online-Durchsuchung und Quellen-Telekommunikationsüberwachung gilt: Das Mittel zur Durchführung dieser Maßnahmen ist die eingesetzte Späh-Software. Diese nutzt lediglich eine Schwachstelle aus. Die Schwachstelle an sich ist nicht das Mittel. Selbst wenn man die Schwachstellen als „Mittel“ im Sinne des § 26a Abs. 2 Satz 2 ASOG ansehen würde, genügt die Norm nicht den oben genannten Mindestanforderungen an ein Schwachstellenmanagement. § 26a Abs. 2 Satz 2 ASOG selbst enthält keine Konkretisierung der zu treffenden Schutzvorkehrungen. Nicht einmal die Gesetzesbegründung konkretisiert, welche Schutzvorkehrungen sich der Gesetzgeber vorgestellt hat bzw. wie diese umzusetzen wären,

vgl. Abgh-Drs. 19/2553, S. 197.

Auch der Regelung über die Datenschutz-Folgenabschätzung in § 53 BlnDSG sind keine Vorgaben zu einem Schwachstellenmanagement zu entnehmen. Mit Blick auf die Tatbestandsvoraussetzungen ist festzustellen, dass das Offenhalten von IT-Schwachstellen keine Verpflichtung zur Datenschutz-Folgenabschätzung auslösen kann und das Schwachstellenmanagement somit nicht vom Tatbestand des § 53 BlnDSG erfasst ist. Weder der Ankauf von Sicherheitslücken noch das Offenhalten in Form eines unterbleibenden Hinweises an Hersteller*innen stellen eine „Verarbeitung“ im Sinne der Norm dar. Zudem würde § 53 BlnDSG aufgrund seiner geringen Regelungsdichte selbst bei unterstellter Anwendbarkeit nicht den aus dem Gebot der Bestimmtheit folgenden Anforderungen an eine einfachgesetzliche Konkretisierung der staatlichen Schutzpflicht genügen.

Auch das sonstige Landesrecht enthält keine hinreichenden Vorgaben. Nach § 23 Abs. 2 Satz 3 EGovG Bln sammelt und bewertet das Computersicherheits-Ereignis- und Reaktionsteam (Berlin-CERT) die zur Abwehr von Gefahren für die Sicherheit der Informationstechnik erforderlichen Daten, insbesondere zu Sicherheitslücken und spricht Warnungen und Handlungsempfehlungen aus. Eine Meldepflicht der Berliner Polizei gibt es jedoch nicht. Diese ergibt sich auch nicht aus § 23 Abs. 2 Satz 2 EGovG Bln. Danach besteht eine Meldepflicht für sicherheitsrelevante Vorfälle (vgl. § 2 Nr. 40 BSIG; Art. 4 Nr. 7 Richtlinie (EU) 2016/1148), nicht für Schwachstellen.

Untergesetzliche Regelungen sind von vorneherein nicht geeignet, den verfassungsrechtlichen Anforderungen zu genügen, da das Schwachstellenmanagement zumindest in Grundzügen in einem formellen Gesetz geregelt sein muss.

III. § 28a ASOG (biometrischer Abgleich mit öffentlich zugänglichen Daten)

§ 28a ASOG verletzt das Recht auf informationelle Selbstbestimmung aus Art. 33 VvB sowie die Versammlungsfreiheit aus Art. 26 VvB.

Die Norm ermächtigt zum Abgleich biometrischer Daten zu Gesichtern und Stimmen mit allgemein öffentlich zugänglichen Daten aus dem Internet (1.). Ein solcher Abgleich setzt grundsätzlich den Aufbau einer

Referenzdatenbank mit biometrischen Daten durch die Polizei selbst oder durch Dritte voraus, kann jedoch (eingeschränkt) auch ohne eine solche dauerhafte Datenbank durchgeführt werden (2.).

Sowohl die Erhebung und Speicherung der öffentlich zugänglichen Daten als auch deren biometrischer Abgleich stellen eigenständige Eingriffe in das Grundrecht auf informationelle Selbstbestimmung dar (3. a)). Diese Eingriffe sind nicht gerechtfertigt (3. b)). Angesichts ihrer hohen Eingriffsintensität genügt § 28a ASOG den verfassungsrechtlichen Anforderungen nicht. Die Norm ermöglicht eine flächendeckende biometrische Durchsuchung des digitalen öffentlichen Raums (3. b) bb) (i)), ohne besonders sensible Daten vom Abgleich auszunehmen (3. b) bb) (ii)). Zudem sind die Voraussetzungen des Abgleichs teilweise unzureichend (3. b) bb) (iii)), auch soweit dieser unverhältnismäßig auf Kontakt- und Begleitpersonen erstreckt wird (3. b) bb) (iv)). Zudem enthält die Norm keine hinreichenden gesetzlichen Schutzvorkehrungen vor Diskriminierung (3. b) bb) (v)). Darüber hinaus verletzt die Vorschrift die Versammlungsfreiheit aus Art. 26 VvB, soweit sie auch den biometrischen Abgleich von Bildern ermöglicht, die im Zusammenhang mit Versammlungen veröffentlicht wurden (4.).

1. Gesetz und Gesetzesbegründung

Der neu eingefügte § 28a schafft eine Rechtsgrundlage für den Abgleich von biometrischen Daten zu Gesichtern und Stimmen mit allgemein öffentlich zugänglichen personenbezogenen Daten aus dem Internet zum Zweck der Identifizierung und der Ermittlung des Aufenthaltsorts von Personen.

Die Norm hat folgenden Wortlaut:

§ 28a

Nachträglicher biometrischer Abgleich mit öffentlich zugänglichen Daten aus dem Internet

(1) Die Polizei kann biometrische Daten zu Gesichtern und Stimmen der in den Nummern 1 bis 3 genannten Personen und deren Kontakt- und Begleitpersonen, auf die sie zur Erfüllung ihrer Aufgaben zugreifen darf, mittels einer automatisierten Anwendung zur Datenverarbeitung zum Zweck der Identifizierung und der Ermittlung des Aufenthaltsorts biometrisch mit allgemein öffentlich zugänglichen personenbezogenen Daten aus dem Internet abgleichen, wenn

1. eine Person nach den §§ 13 oder 14 verantwortlich ist für eine Gefahr für

a) den Bestand oder die Sicherheit des Bundes oder eines Landes,

b) Leib, Leben oder Freiheit einer Person,

c) die sexuelle Selbstbestimmung einer Person, soweit sie durch Straftatbestände geschützt ist, bei denen die Tat mit Freiheitsstrafe nicht unter sechs Monaten bedroht ist, oder

d) Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist,

2. tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass eine Person innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise

a) eine terroristische Straftat oder

b) eine in § 100b Absatz 2 der Strafprozessordnung genannte und voraussichtlich auch im Einzelfall besonders schwerwiegende Straftat

begehen oder an ihr teilnehmen wird, oder

3. das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums eine terroristische Straftat begehen oder an ihr teilnehmen wird.

Die Maßnahmen sind nur zulässig, wenn die Abwehr der Gefahr oder die Verhütung der Straftat auf andere Weise aussichtslos oder wesentlich erschwert wäre und die jeweilige Maßnahme nicht außer Verhältnis zur Bedeutung des aufzuklärenden Sachverhalts steht. Allgemein öffentlich zugängliche personenbezogene Daten aus dem Internet dürfen zu diesem Zweck erhoben, gespeichert und aufbereitet werden.

(2) Für die mit Maßnahmen nach Absatz 1 Satz 1 abzugleichenden Daten gilt § 42a Absatz 2 und 3 entsprechend. Maßnahmen nach Absatz 1 Satz 1, die sich auf im Internet öffentlich zugängliche Echtzeit-Lichtbild- und Echtzeit-Videodateien beziehen, sind unzulässig.

(3) Führt eine Maßnahme nach Absatz 1 Satz 1 zu einer Datenübereinstimmung, so dürfen weitere Maßnahmen erst nach Identifikation der betroffenen Person durch Inaugenscheinnahme erfolgen. Führt eine Maßnahme nach Absatz 1 Satz 1 nicht zu einer Datenübereinstimmung oder kann die Datenübereinstimmung durch die in Satz 1 vorgesehene Überprüfung nicht bestätigt werden, sind die erhobenen Daten sofort technisch spurlos und im Fall einer bereits nach erfolgter Durchführung eines Datenabgleichs nach Absatz 1 fehlenden Datenübereinstimmung automatisiert zu löschen.

(4) Maßnahmen nach Absatz 1 Satz 1 bedürfen der gerichtlichen Anordnung, die von der Polizeipräsidentin oder dem Polizeipräsidenten oder der Vertretung im Amt zu beantragen ist; diese Befugnis kann von der Polizeipräsidentin oder dem Polizeipräsidenten auf die Leitung des Landeskriminalamtes und die Vertretung im Amt übertragen werden. Bei Gefahr im Verzug kann die Anordnung durch die Polizeipräsidentin oder den Polizeipräsidenten oder die Vertretung im Amt getroffen werden. Die gerichtliche Bestätigung der Anordnung ist in diesem Fall unverzüglich einzuholen. Die Anordnung tritt außer Kraft, wenn sie nicht binnen drei Werktagen gerichtlich bestätigt wird. In diesem Fall dürfen die bereits

erhobenen Daten nicht mehr verwendet werden; sie sind unverzüglich zu löschen und die Löschung ist zu protokollieren. Sind bereits Daten übermittelt worden, die nach Satz 5 zu löschen sind, so ist die empfangende Stelle darüber zu unterrichten.

(5) Maßnahmen nach Absatz 1 Satz 1 dürfen nur von ausgewählten und geschulten Polizeidienstkräften durchgeführt werden. Nach Beendigung der Maßnahme ist die oder der behördliche Datenschutzbeauftragte zu unterrichten. Lässt die Polizei Maßnahmen nach Absatz 1 durch Auftragsverarbeitende oder zur Verarbeitung eingesetzte Dritte durchführen, ist § 42d Absatz 3 Satz 3 bis 8 entsprechend anzuwenden.

(6) Verwaltungsvorschriften bestimmen das Nähere insbesondere

1. hinsichtlich des Verfahrens nach Absatz 1 Satz 1 zu

a) dem technischen Verfahren nach Absatz 1,

b) der Eingabe- und Zugangsberechtigung,

c) den sonstigen Sicherungsmaßnahmen zur Verhinderung unbefugter Datenzugriffe,

d) den Speicher- und Löschfristen,

e) der Art der zu speichernden Daten,

f) dem Personenkreis, der von der Speicherung betroffen ist,

g) der Dauer der Speicherung,

h) der Protokollierung sowie

2. hinsichtlich des Verfahrens nach Absatz 1 Satz 3 zu Art, Umfang und Dauer einer Speicherung der abzugleichenden, öffentlich zugänglichen Lichtbild-, Video- und Audiodateien.

Die Verwaltungsvorschriften treten an die Stelle der Errichtungsanordnung nach § 49. Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit ist vor dem Erlass oder einer Änderung der Verwaltungsvorschriften anzuhören. Die Verwaltungsvorschriften sind zu veröffentlichen.“

Die Gesetzesbegründung nennt als Anlass für die Einführung der Befugnis den Fall der mutmaßlichen Terroristin Daniela Klette. Es seien investigativ tätige Journalisten gewesen, welche die alten Fahndungsfotos aus den 90er Jahren durch künstliche Intelligenz mit öffentlich zugänglichen Fotos aus dem Internet abglichen und so entscheidende Hinweise auf den aktuellen Aufenthaltsort von Frau Klette hätten geben können. Dieser Fall habe deutlich gezeigt, welcher Nachholbedarf hier für die Polizei bestehe. Das gelte nicht nur im Bereich der Strafverfolgung, sondern auch bei der Gefahrenabwehr,

Abgh-Drs. 19/2553, S. 236.

Der biometrische Abgleich öffentlich zugänglicher Daten erfolge mithilfe der KI automatisiert, denn nur durch technische Anwendungen könnten Lichtbilder und Videos in einer Form zusammengeführt und analysiert werden, die einen schnellen und wirkungsvollen Abgleich ermögliche. Das erfordere eine Befugnisnorm, die methodenoffen ausgestaltet ist. Denn die technischen Möglichkeiten für die biometrische Fernidentifizierung, auch durch KI-Einsatz, entwickelten sich in rasanter Weise weiter. Die vorgeschlagene Regelung orientiere sich am Gesetz zur Verbesserung der Terrorismusbekämpfung, das der Deutsche Bundestag am 18. Oktober 2024 beschlossen habe, aber nicht in Kraft getreten sei, weil ihm der Bundesrat die erforderliche Zustimmung versagt habe,

Abgh-Drs. 19/2553, S. 236 mit Verweisen auf BR-Drs 512/24 zur BT-Drs. 20/12806.

Durch den Änderungsantrag der Fraktionen der CDU und der SPD wurde die Norm teilweise geändert. Insbesondere wurde zusätzlich der Abgleich von Daten von Kontakt- und Begleitpersonen ermöglicht und Absatz 3 eingefügt, der unter anderem die Löschung bei fehlenden Übereinstimmungen regelt,

Änderungsantrag der Fraktion der CDU und der Fraktion der SPD zur Drucksache 19/2553, **Anlage 6**, S. 10 und S. 34.

2. Funktionsweise und Anwendungsszenarien

Der Abgleich ist grundsätzlich auf drei verschiedene Weisen möglich.

Erstens besteht technisch die Möglichkeit eines Abgleichs gegen eine bereits aufgebaute biometrische Datenbank (One-to-many-Abgleich). Hier wird aus dem Referenzbild (etwa aus einer Überwachungskamera) zunächst ein biometrisches Template erstellt. Dieses wird anschließend mit einer bereits vorhandenen Datenbank biometrischer Templates verglichen, die zuvor aus Internetbildern gewonnen und indexiert wurde. Dies entspricht der Arbeitsweise spezialisierter Gesichtserkennungssysteme wie PimEyes oder Clearview AI: Die Bilder werden zuvor gesammelt (Crawling), biometrisch vorverarbeitet (Template-Erstellung) und in einer durchsuchbaren Datenbank

gespeichert. Erst dadurch wird ein schneller One-to-many-Abgleich möglich,

Lewandowski, Braucht die Polizei eine Datenbank zum biometrischen Abgleich? Das Durchsuchen von Internetbildern zur Gesichtserkennung, September 2025, abrufbar unter <https://algorithmwatch.org/de/gutachten-datenbank-biometrie-gesichtserkennung/>, S. 12 ff.

Es ist jedoch zweifelhaft, ob dieses Vorgehen nach dem vorliegenden Gesetz zulässig ist. Nach § 28a Abs. 3 Satz 2 ASOG sind die erhobenen Daten sofort technisch spurlos zu löschen, wenn der Abgleich nicht zu einer Datenübereinstimmung führt oder die Datenübereinstimmung durch die Inaugenscheinnahme nicht bestätigt werden kann. Dies dürfte dem Aufbau einer eigenen Referenzdatenbank entgegenstehen. Abgesehen dürfte der Aufbau einer solchen Referenzdatenbank gegen Art. 5 Abs. 1 e) KI-VO verstoßen,

vgl. Teichmann, NJOZ 2026, 705 Rn. 15 ff.

Denkbar ist jedoch, zweitens, dass die Polizei für jeden Abgleich Daten bei einem privaten Dritten erhebt, der zuvor eine solche Referenzdatenbank aufgebaut hat. Die Polizei würde gewissermaßen für jeden Abgleich eine Referenzdatenbank kaufen und sie anschließend wieder löschen. § 28 Abs. 1 Satz 3 ASOG steht dem nicht entgegen. Danach dürfen allgemein öffentlich zugängliche personenbezogene Daten aus dem Internet zum Zwecke des Abgleichs erhoben, gespeichert und aufbereitet werden. Wo sie erhoben werden, ist nicht geregelt. Sie müssen insbesondere nicht durch eigenes sogenanntes „Crawling“ im Internet selbst erhoben werden, sondern können auch von Dritten „angekauft“ werden, solange sichergestellt ist, dass es sich um allgemein öffentlich zugängliche personenbezogene Daten aus dem Internet handelt. Der Dritte ist in diesem Szenario auch nicht zwingend ein Auftragsverarbeiter, so dass die Beschränkung auf innereuropäische Anbieter nach § 28a Abs. 5 Satz 3 ASOG nicht greift. In diesem Szenario könnte theoretisch sogar die Referenzdatenbank von PimEyes oder Clearview AI gekauft und für den Abgleich genutzt werden.

Alternativ könnte, drittens, versucht werden, bei jeder einzelnen Anfrage das Internet oder bestimmte Internetquellen unmittelbar zu durchsuchen (sogenannter „Live“-Abgleich ohne Datenbank). Dabei müsste jedes gefundene Bild heruntergeladen, daraus ein biometrisches Template erzeugt, dieses mit dem Referenzbild verglichen und anschließend wieder gelöscht werden (One-to-One-Abgleich). Ein dauerhafter Datenbestand würde dabei nicht entstehen. Ein solcher Ansatz wird als unpraktikabel beschrieben, da er sehr zeitaufwändig ist,

Lewandowski, Braucht die Polizei eine Datenbank zum biometrischen Abgleich? Das Durchsuchen von Internetbildern zur Gesichtserkennung, September 2025, abrufbar unter <https://algorithmwatch.org/de/gutachten-datenbank-biometrie-gesichtserkennung/>, S. 12 ff.

Bei hohen Rechnerkapazitäten und langer Dauer können dennoch große Datenmengen abgeglichen werden.

In beiden grundsätzlich zulässigen Varianten können (innereuropäische) private Anbieter mit der Durchführung des Abgleichs beauftragt werden (§ 28a Abs. 5 Satz 3 ASOG i.V.m. § 42d Abs. 3 Satz 3 ASOG). Der Auftragsverarbeiter wäre jedoch gemäß § 28a Abs. 3 Satz 2 ASOG ebenfalls zur sofortigen Löschung verpflichtet und könnte daher – im Rahmen der Auftragsverarbeitung – keine Referenzdatenbank aufbauen. Dies berührt jedoch nicht die oben genannte Möglichkeit, die Referenzdatenbank von einem (anderen) Dritten anzukaufen oder losgelöst von der Auftragsverarbeitung eine Referenzdatenbank aufzubauen.

3. Verstoß gegen Art. 33 VvB

§ 28a ASOG verletzt das Recht auf informationelle Selbstbestimmung. Die mit der Datenverarbeitung verbundenen Eingriffe in das Recht des einzelnen nach Art. 33 VvB, grundsätzlich selbst über die Verwendung seiner persönlichen Daten zu bestimmen (a)), sind nicht gerechtfertigt (b)).

a) Eingriffe in den Schutzbereich

Die biometrischen Daten zu Gesichtern und Stimmen sind persönliche Daten im Sinne des Art. 33 VvB. Der Schutzbereich ist daher eröffnet,

zum Schutzbereich siehe oben I. 3.

Ein Grundrechtseingriff liegt zunächst darin, dass allgemein öffentlich verfügbare Daten aus dem Internet erhoben und gespeichert werden. An der Eingriffsqualität fehlt es lediglich, sofern Daten ungezielt und allein technikbedingt zunächst miterfasst, aber unmittelbar nach der Erfassung technisch wieder anonym, spurenlos und ohne Erkenntnisinteresse für die Behörden ausgesondert werden. Demgegenüber kann auch dann, wenn die Erfassung eines größeren Datenbestands letztlich nur Mittel zum Zweck für eine weitere Verkleinerung der Treffermenge bildet, in der Datenerhebung als solcher bereits ein Eingriff liegen. Maßgeblich ist, ob sich bei einer Gesamtbetrachtung mit Blick auf den durch den Überwachungs- und Verwendungszweck bestimmten Zusammenhang das behördliche Interesse an den betroffenen Daten bereits derart verdichtet hat, dass ein Betroffensein in einer einen Grundrechtseingriff auslösenden Qualität zu bejahen ist,

BVerfGE 150, 244 <266 Rn. 43>.

Bei der Erhebung und Speicherung von Daten zum Zwecke des biometrischen Abgleichs ist eine solche Verdichtung – wie bei der automatisierten Kennzeichenerfassung – gegeben,

vgl. BVerfGE 150, 244 <267 f. Rn 47 ff.>.

Ein weiterer Eingriff liegt in dem Abgleich der Daten sowie in der folgenden Verwendung der gefilterten Daten,

vgl. BVerfGE 150, 244 <266 Rn 44>; Hahn, Automatisierte Gesichtserkennung in der Strafverfolgung, 2025, S. 101 ff.

b) Keine Rechtfertigung

Die Eingriffe sind nicht gerechtfertigt.

Der nachträgliche biometrische Abgleich von personenbezogenen Daten mit öffentlich zugänglichen Daten aus dem Internet dient zwar einem legitimen Zweck und kann auch geeignet und erforderlich sein.

§ 28a ASOG genügt jedoch nicht dem Gebot der Verhältnismäßigkeit im engeren Sinne. Die Erhebung der Daten und der daran

anschließende Abgleich sind Eingriffe von hoher Intensität (aa)), die nur unter sehr engen Voraussetzungen angemessen sind. Diese Voraussetzungen müssen hinreichend bestimmt und normenklar im Gesetz selbst festgelegt sein. Das ist nicht der Fall (bb)).

aa) Eingriffsintensität

Der Maßnahmen greifen tief in Grundrechte ein. Dies ergibt sich aus der Streubreite ((i)), der Art der Daten ((ii)), der Verarbeitungsdauer ((iii)), der potenziellen Folgen der Verarbeitung ((iv)), der Risiken der Nutzung künstlicher Intelligenz ((v)) und der Heimlichkeit der Maßnahme ((vi)),

vgl. zum Folgenden auch Hahn, Automatisierte Gesichtserkennung in der Strafverfolgung, 2025, S. 107 ff.

(i) Streubreite

Der Eingriff hat eine immense Streubreite. Es werden nicht nur die biometrischen Daten der Polizeiverantwortlichen und deren Kontakt- und Begleitpersonen verarbeitet,

vgl. zu der damit verbundenen Streubreite: Berliner Beauftragte für Datenschutz und Informationsfreiheit, Stellungnahme zum Änderungsantrag der Fraktion der CDU und der Fraktion der SPD zur Drucksache 19/2553: Gesetz zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 7**, S. 1 f.,

sondern insbesondere auch die biometrischen Daten, mit denen der Abgleich durchgeführt wird. Das können alle Personen sein, deren Gesichter oder Stimmen im Internet allgemein öffentlich zugänglich sind. Dies führt dazu, dass in die Grundrechte von einer unbegrenzten Vielzahl von unbeteiligten Personen eingegriffen wird,

vgl. Rückert, StV 2025, 350.

Das Bundesverfassungsgericht führt hierzu in seiner Entscheidung zur Kennzeichenerfassung aus:

„Das Eingriffsgewicht erhöhend zeichnen sich solche Kontrollen dadurch aus, dass sie sich schon ihrem Prinzip nach nicht auf Personen beschränken, die objektiv in einer Gefahrenlage verfangen sind, sondern sich auf eine unbestimmte Vielzahl von Personen erstrecken, die von vornherein hierzu keinerlei Anlass gegeben haben. Sie können praktisch jede und jeden treffen. Solche

Informationserhebungen haben grundsätzlich eine erhöhte Eingriffsintensität.“

BVerfGE 150, 244 <283 f. Rn. 98>.

Es ist von einer hohen Gesamtzahl der erfassten Personen auszugehen,

vgl. BVerfGE 115, 320 <357 Rn. 123 f.>.

Das gilt unabhängig davon, ob für den Abgleich auf eine Referenzdatenbank zurückgegriffen wird oder ein One-to-One-Abgleich erfolgt. Auch bei einem One-to-One-Abgleich können große Mengen an sensiblen Daten verarbeitet werden.

(ii) Art der Daten

Das Eingriffsgewicht wird nur unwesentlich dadurch gemindert, dass die Daten, mit denen der Abgleich durchgeführt wird, allgemein öffentlich zugänglich sein müssen. Da einzelne Personen nur begrenzt beeinflussen können, ob Bild- und Videomaterial von ihnen im Internet veröffentlicht wird, sind davon potenziell alle Menschen betroffen. Insbesondere ist inzwischen üblich, Fotos und Videos von privaten oder öffentlichen Zusammenkünften auf Social-Media-Plattformen zu veröffentlichen. Das Einverständnis der betroffenen Personen wird in den seltensten Fällen eingeholt,

vgl. zum Zugriff auf Daten, die ohne Einwilligung veröffentlicht wurden Rückert, StV 2025, 350 (351).

Es kommt zudem vor, dass Kriminelle auf unveröffentlichte Gesichtsbilder und Stimmufnahmen zugreifen und sie veröffentlichen,

vgl. swr.de vom 22. Mai 2026, Kinderbilder von Plattform gestohlen - Das ist bekannt, <https://www.swr.de/swraktuell/rheinland-pfalz/hacker-klauen-fotos-und-daten-von-kita-und-schulkindern-cybertacke-auf-portraitbox-100.html>.

Auch wenn ein Foto von der betroffenen Person selbst eingestellt wird, wird die Schutzwürdigkeit nicht wesentlich gemindert. Eine eigene Präsenz (mit Foto) auf gängigen Social-Media-Plattformen wie TikTok, Instagram, Facebook oder LinkedIn ist inzwischen üblich und in vielen Kreisen eine Bedingung für die Teilhabe am gesellschaftlichen Leben. Wer als junge Person keinen TikTok- oder Instagram-Account hat,

verpasst wichtige Aktivitäten. Wer auf Jobsuche ist, hat es ohne LinkedIn-Profil schwerer. Auch die Teilnahme am Prozess der politischen Meinungsbildung erfolgt zunehmend über Social Media,

vgl. BVerfG, Beschluss des Ersten Senats vom 1. Oktober 2025 – 1 BvR 2428/20 –, Rn. 71.

Hinzu kommt, dass im Internet einmal veröffentlichte Daten nur schwer wieder zu löschen sind. Selbst wenn die ursprüngliche Seite nicht mehr verfügbar ist, finden sich die Dokumente oft in Internetarchiven und sind beispielsweise über die sogenannte „Wayback Machine“ unter archive.org weiter abrufbar. Sie stehen daher auch weiterhin für den automatisierten Abgleich zur Verfügung.

Die Daten sind auch sensibel. Dies folgt zunächst allgemein daraus, dass biometrische Daten verarbeitet werden,

vgl. BVerfG, Urteil des Ersten Senats vom 16. Februar 2023 – 1 BvR 1547/19 –, Rn. 87

Biometrische Daten sind mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten (Art. 4 Nr. 14 DSGVO; § 31 Nr. 12 BlnDSG). Wegen der Möglichkeit der eindeutigen Identifizierung sind sie besonders sensibel und werden entsprechend auch besonders geschützt (vgl. Art. 9 DSGVO; § 33 BlnDSG).

Eingriffsintensivierend wirkt sich außerdem aus, dass im Rahmen des – nach der Speicherung in einer Datenbank – geplanten biometrischen Abgleichs, neben der Identifizierung der Person auch Rückschlüsse auf weitergehende sensible Informationen ermöglicht werden, wie beispielsweise die politische Einstellung (z.B. Bilder von Parteiveranstaltungen) oder die sexuelle Orientierung (z.B. Bilder auf queeren Dating-Plattformen) der betroffenen Person,

vgl. Ogorek, LTZ 2024, 274 (278).

Von dem automatisierten Abgleich sind auch Bilder von Versammlungen erfasst, die etwa von der (digitalen) Presse veröffentlicht werden. Die Veröffentlichung solcher Bilder ist legal (vgl. § 23 Abs. 1 Nr. 3 KUG). Betroffene können sich wegen des Vermummungsverbots (vgl. für Berlin § 19 Abs. 1 Nr. 1 VersFG) nicht vor einer Erfassung des Gesichts schützen. Die Befugnis zum biometrischen Abgleich kann Menschen davon abhalten, von ihrer Versammlungsfreiheit Gebrauch zu machen,

vgl. BVerfGE 65, 1 <43 Rn. 154>; BVerfG, Beschluss des Ersten Senats vom 17. Februar 2009 – 1 BvR 2492/08 –, Rn. 131; Ogorek, LTZ 2024, 274 (278).

Es ist auch nicht ausgeschlossen, dass Erkenntnisse aus dem Kernbereich privater Lebensgestaltung durch die Maßnahme erlangt werden. In diesem Zusammenhang ist beispielsweise an Dating-Plattformen sowie an die Vielzahl sensibler Aufnahmen zu denken, die oftmals auch ohne Einverständnis der abgebildeten Personen erstellt und im Internet veröffentlicht werden (z.B. sogenannter Rache-Porno).

Je nach Umfang des Datenabgleichs, der unbegrenzt durch die Norm ermöglicht wird, lassen sich mit hoher Wahrscheinlichkeit umfassende Bewegungs- und Persönlichkeitsprofile erstellen, wie bereits angemerkt ebenfalls für Kontakt- und Begleitpersonen.

Die in § 28a Abs. 2 Satz 2 ASOG ausgeschlossene Echtzeit-Überwachung schränkt die Art der im Datenabgleich verwendeten Daten nicht wesentlich ein. Zwar fällt danach ein geringer Teil der im Internet zugänglichen Daten wie „Live-Material“ oder „Near-live-Material“ aus dem Abgleich heraus. Im Zweifel ist der nachträgliche Abgleich von biometrischen Daten indes sogar eingriffsintensiver, denn anders als bei einer reinen Echtzeit-Überwachung, kann durch einen nachträglichen Abgleich von Daten aus den letzten Wochen, Monaten oder Jahren, ein ganzes Bewegungs- oder Persönlichkeitsprofil der betroffenen Person erstellt werden,

vgl. Berliner Beauftragte für Datenschutz und Informationsfreiheit, Stellungnahme zum Gesetzentwurf zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 2**, S. 13.

Ein entsprechender Ausschluss der Echtzeitüberwachung für Stimmen fehlt gänzlich.

(iii) Verarbeitungsdauer

Die Löschpflicht nach § 28a Abs. 3 Satz 2 ASOG reduziert das Eingriffsgewicht. Insbesondere ist dadurch ausgeschlossen, dass die Polizei selbst eine Referenzdatenbank auf Vorrat aufbaut. Allerdings ist das Eingriffsgewicht auch bei einer kurzzeitigen Erhebung und Verarbeitung hoch. Zudem besteht die Gefahr, dass die Polizei Referenzdatenbanken bei Dritten kauft und so illegalen Praktiken Vorschub leistet,

siehe oben 2.

(iv) Folgen des Abgleichs

Die Folgen des Abgleichs können schwerwiegend sein. Zwar sieht § 28a Abs. 3 Satz 1 ASOG vor, dass weitere Maßnahmen erst nach Identifikation der betroffenen Person durch Inaugenscheinnahme erfolgen dürfen. Jedoch besteht beim biometrischen Abgleich eine größere Gefahr des oben beschriebenen „Automation Bias“,

siehe dazu oben I. 4. a) bb) (ii),

weil die biometrische Gesichtserkennung scheinbar weniger fehleranfällig ist als die Verhaltenserkennung. Gleichzeitig ist die absolute Anzahl der abgeglichenen Bilder (potenziell) so hoch, sodass auch bei einer niedrigen Falsch-Positiv-Rate in absoluten Zahlen viele Fehler anfallen. Wer – möglicherweise unzutreffend – von der Software erkannt wird, wird mit hoher Wahrscheinlichkeit Adressat oder Adressatin von polizeilichen Folgemaßnahmen (z.B. Observationen, Telekommunikationsüberwachungen, Festnahmen).

(v) Risiken durch künstliche Intelligenz

Die Tragweite des Eingriffs wird durch den Einsatz künstlicher Intelligenz (KI) noch verstärkt,

vgl. Rückert, StV 2025, 350 (351); zu den Gefahren der künstlichen Intelligenz bereits oben I. 4.a) bb) (i).

Der biometrische Abgleich soll mithilfe von KI automatisiert erfolgen, da nur durch technische Anwendungen Lichtbilder und Videos in einer

Form zusammengeführt und analysiert werden können, die einen schnellen und wirkungsvollen Abgleich ermöglicht,

vgl. Abgh-Drs. 19/2553, S. 236.

Diese automatisierte Massenauswertung potenziert die Eingriffsintensität erheblich, auch wegen ihrer Fehleranfälligkeit und des Diskriminierungspotentials,

vgl. Berliner Beauftragte für Datenschutz und Informationsfreiheit, Stellungnahme zum Gesetzentwurf zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 2**, S. 12.

Auch der aktuelle Stand der Forschung geht weiterhin davon aus, dass automatisierte Gesichtserkennung je nach demographischer Gruppe unterschiedlich hohe Fehlerraten aufweist. Unabhängige Evaluierungen des US National Institute of Standards and Technology (NIST) bestätigen fortbestehende Unterschiede insbesondere hinsichtlich ethnischer Herkunft, Geschlecht und Alter. Diese Unterschiede können zu diskriminierenden Fehlidentifizierungen führen und lassen sich durch technische Verbesserungen bislang nicht vollständig beseitigen,

vgl. Grother u.a., Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, 2019; siehe auch die aktuellen Zahlen auf https://pages.nist.gov/frvt/html/frvt_demographics.html.

(vi) Heimlichkeit

Das Eingriffsgewicht wird schließlich dadurch erhöht, dass der Abgleich weitgehend verdeckt durchgeführt wird. Auch insofern ist die Maßnahme mit der automatisierten Kennzeichenerfassung vergleichbar:

„Weiter fällt belastend ins Gewicht, dass die Maßnahmen verdeckt durchgeführt werden. Gerade bei Ermittlungsmaßnahmen mit großer Streubreite wie hier der im öffentlichen Raum stattfindenden seriellen Kontrolle von Personen in großer Zahl zu Fahndungszwecken kann dadurch ein Gefühl des Überwachtwerdens entstehen. Dass die von der Kennzeichenkontrolle erfassten Personen dies außerhalb des Trefferfalls nicht bemerken, hebt das hierin liegende Eingriffsgewicht nicht auf. Denn dadurch entfällt zwar die Lästigkeit solcher Maßnahmen, nicht aber ihr Kontrollcharakter und die darin liegende Beeinträchtigung der individuellen Freiheit, die zugleich die Freiheitlichkeit der Gesellschaft insgesamt betrifft.“

BVerfGE 150, 244 <283 f. Rn. 98>.

Eine Benachrichtigung nach § 27d Abs. 1 ASOG erfolgt nur, wenn personenbezogene Daten „erlangt“ werden, also nur bei Treffern.

bb) Verletzung der verfassungsrechtlichen Anforderungen

Die hohe Eingriffsintensität hat zur Folge, dass der biometrische Abgleich nur unter engen Voraussetzungen gerechtfertigt werden kann.

Dabei ist der Grundsatz der Bestimmtheit und Normenklarheit zu beachten, nach dem an Ermächtigungen zur heimlichen Erhebung und Verarbeitung von Daten besonders strenge Anforderungen zu stellen sind. Es ist Aufgabe des parlamentarischen Gesetzgebers, die Voraussetzungen und den Umfang heimlicher Überwachungsbefugnisse zu regeln,

BVerfG, Beschluss des Ersten Senats vom 14. November 2024 – 1 BvL 3/22 –, Rn. 85 f. m.w.N.

Diesen Anforderungen genügt § 28a ASOG nicht. Die Norm verstößt gegen das Verbot flächendeckender Überwachung im digitalen Raum ((i)). Sie ist zudem unverhältnismäßig, weil sensible Daten nicht vom Abgleich ausgenommen sind ((ii)), die Anforderungen an Rechtsgüterschutz und Eingriffsschwellen nicht durchgehend erfüllt sind ((iii)), der Abgleich nicht auf Polizeiverantwortliche beschränkt ist ((iv)) und es an konkreten Schutzvorkehrungen gegen Diskriminierung fehlt ((v)).

(i) Verstoß gegen das Verbot flächendeckender Überwachung

Zunächst folgt aus dem Verhältnismäßigkeitsgrundsatz, dass nicht sämtliche im Internet allgemein öffentlich verfügbaren Daten für den Abgleich verarbeitet werden dürfen. Dies ermöglicht– bis auf wenige Ausnahmen für Live-Material – indes § 28a ASOG.

Die Maßnahme weist insofern eine Ähnlichkeit zur Kennzeichenerfassung auf. Hier hat das Bundesverfassungsgericht entschieden, dass Maßnahmen nicht flächendeckend durchgeführt werden dürfen,

BVerfGE 150, 244 <285 f. Rn. 100>.

Die bayerischen Regelungen waren nur deshalb verhältnismäßig, weil Art. 33 Abs. 2 Satz 5 BayPAG a.F. regelte, dass die Maßnahmen nicht flächendeckend eingesetzt werden dürfen:

„Gemeint ist hiermit, dass die Kontrollen nur an einzelnen erfolgversprechenden Stellen, das heißt punktuell örtlich begrenzt durchgeführt werden dürfen, nicht aber zu dem Zweck, kontrollfreie Bewegungen möglichst weiträumig oder gar im gesamten Zuständigkeitsbereich der Behörde auszuschließen.“

BVerfGE 150, 244 <289 Rn. 115>.

Die Kontrollen an „gefährlichen Orten“ sind beschränkt auf „Orte, für die tatsächliche Anhaltspunkte bestehen, dass sie von den in der Vorschrift genannten Personen [insb. Straftäter] maßgeblich frequentiert werden“,

BVerfGE 150, 244 <290 Rn. 120>.

Der Zweck des Verbots flächendeckender Überwachung besteht darin, zu verhindern, dass der Staat ohne hinreichenden Anlass den gesamten öffentlichen Raum kontrolliert. Dieses Schutzanliegen gilt für den biometrischen Datenabgleich im digitalen Raum in mindestens gleicher, wenn nicht sogar stärkerer Weise. Während sich die Kennzeichenerfassung auf den Straßenverkehr beschränkt, ermöglicht der Abgleich mit allgemein öffentlich zugänglichen Internetdaten die Durchsuchung praktisch des gesamten digitalen öffentlichen Raums. Die Eingriffsstreubreite ist deshalb sogar größer als bei der Kennzeichenerfassung. Zudem sind biometrische Daten sensibler als Kennzeichen.

Überträgt man das Verbot flächendeckender Überwachung auf den digitalen Raum, bedeutet dies, dass nur solche Teile des Internets für den Datenabgleich genutzt werden dürfen, in denen eine gesteigerte Wahrscheinlichkeit von Treffern besteht. Bei einem geplanten rechtsterroristischen Anschlag wäre es etwa verhältnismäßig, einen biometrischen Abgleich mit den Fotos aus (öffentlichen) rechtsextremen Chatgruppen durchzuführen.

Dass ein solcher Abgleich damit weniger effektiv ist als die Nutzung von kommerziellen Angeboten wie PimEyes, ist konsequent. Denn

eigentlich dürfte es Angebote wie die von Clearview AI und PimEyes gar nicht geben. Sie verstoßen eindeutig gegen Art. 9 Abs. 1 DSGVO,

Hornung/Schindler, DuD 2021, 515 (518 ff.).

Es fehlt lediglich an einer effektiven Rechtsdurchsetzung. Der Landesbeauftragte für Datenschutz Baden-Württemberg hat 2022 zwar ein Bußgeldverfahren gegen PimEyes eröffnet. Das Unternehmen hat seitdem jedoch mehrfach den angegebenen Sitz gewechselt. Aktuell soll es seinen Sitz in Dubai haben,

LfDI Baden-Württemberg, PimEyes: LfDI eröffnet Bußgeldverfahren, 21. Dezember 2022, <https://www.baden-wuerttemberg.datenschutz.de/pimeyes-lfdi-eroeffnet-bussgeldverfahren/>; Euraktiv vom 30. April 2026, Failure to tackle facial recognition firm triggers privacy complaint, <https://www.euractiv.com/news/failure-to-tackle-facial-recognition-firm-triggers-privacy-complaint/>.

§ 28a Abs. 1 Satz 1 ASOG erlaubt einen biometrischen Datenabgleich „mit allgemein öffentlich zugänglichen personenbezogenen Daten aus dem Internet“. Der Wortlaut ermöglicht folglich, den gesamten digitalen öffentlichen Raum nach potenziellen Treffern zu durchsuchen. Eine räumliche Konkretisierung durch die Begrenzung der Suche auf Teile des Internets fehlt. § 28a ASOG ist mithin nicht hinreichend begrenzt und mit Blick auf das Recht auf informationeller Selbstbestimmung unverhältnismäßig.

(ii) Kein Ausschluss von sensiblen Daten

Neben dem Verbot einer flächendeckenden Erfassung muss technisch sichergestellt werden, dass sensible Daten nicht für den Abgleich herangezogen werden,

vgl. zu ähnlichen Anforderungen zur Ausfilterung sensibler Daten im Rahmen der strategischen Fernmeldeaufklärung durch den BND BVerfGE 154, 152 <283 Rn. 256>.

Hierzu zählen etwa Daten, die den Kernbereich privater Lebensgestaltung berühren, Fotos von Versammlungen und religiösen Veranstaltungen sowie Daten, die Rückschlüsse auf die sexuelle Orientierung zulassen.

Insbesondere die Verarbeitung von Bildern, die auf Versammlungen entstanden sind, ist mit Blick auf die Bedeutung und Wahrnehmung der verfassungsrechtlich garantierten Versammlungsfreiheit (Art. 26 VvB) unverhältnismäßig. Denn die Möglichkeit der behördlichen Kenntnisnahme über die politische Einstellung einzelner Personen ist geeignet, diese abzuschrecken und von einer zukünftigen Teilnahme an Versammlungen und der damit verbundenen Mitwirkung am politischen Prozess abzuhalten.

§ 28a ASOG begrenzt die Art der Daten, die in den Datenabgleich mit einbezogen werden dürfen, nicht. Es fehlt insbesondere an einer Vorschrift, die sichergestellt, dass besonders sensible Daten nicht in den Abgleich mit aufgenommen werden. Stattdessen erstreckt sich der Wortlaut von § 28a Abs. 1 Satz 1 ASOG auf sämtliche im Internet öffentlich zugängliche Daten, also auch auf besonders persönlichkeitsrelevante, sensible Daten wie solche, die auf Dating-Plattformen veröffentlicht wurden oder im Rahmen von einer Versammlungsteilnahme entstanden sind. Anders als in § 15b Abs. 2 AsylG fehlt es auch an einer auf die Maßnahme zugeschnittenen Vorschrift zum Schutz des Kernbereichs privater Lebensgestaltung.

Im Unterschied zu anderen Normen – z.B. §§ 42c Abs. 5 Satz 1 Nr. 2, 42d Abs. 2 Satz 3 oder 47a Abs. 4 Satz 5 ASOG – enthält § 28a ASOG auch nicht einmal einen Verweis auf § 51a Abs. 2 ASOG. Danach gelten bei der Verarbeitung von besonderen Kategorien personenbezogener Daten, worunter auch biometrische Daten fallen (§ 31 Nr. 14 b) BlnDSG), spezielle Vorkehrungen. Nach § 51a Abs. 2 Satz 2 ASOG sind die an der Verarbeitung Beteiligten für die besondere Schutzbedürftigkeit dieser Daten zu sensibilisieren.

(iii) Unzureichende Voraussetzungen des Abgleichs

Auch die Voraussetzungen des Abgleichs selbst genügen nicht dem Verhältnismäßigkeitsgrundsatzes. Da der Abgleich sehr intensiv in Grundrechte eingreift, ist eine mindestens konkretisierte Gefahr für besonders gewichtige Rechtsgüter erforderlich.

Soweit § 28a Abs. 1 Satz 1 Nr. 2 lit. b) ASOG auf den Straftatenkatalog des § 100b Abs. 2 StPO verweist, genügt die Norm nicht den

Anforderungen an den Rechtsgüterschutz und die Eingriffsschwelle.
Zudem ist die dynamische Verweisung unzulässig,

siehe oben II. 4. b) cc).

(iv) Keine Beschränkung auf Polizeiverantwortliche

Der Abgleich ist zudem auf Polizeiverantwortliche zu beschränken.
Kontakt- und Begleitpersonen dürfen angesichts der Schwere des Grundrechtseingriffs nicht gezielt gesucht werden,

vgl. Berliner Beauftragte für Datenschutz und Informationsfreiheit,
Stellungnahme zum Änderungsantrag der Fraktion der CDU und der
Fraktion der SPD zur Drucksache 19/2553: Gesetz zur Reform des
Berliner Polizei- und Ordnungsrechts und zur Änderung des
Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 7**, S. 1 f.,

Allenfalls kommt eine Suche nach Kontakt- und Begleitpersonen in
Betracht, wenn der Abgleich von Daten des Verantwortlichen erfolglos
geblieben ist oder ausscheidet (Subsidiarität),

vgl. zur Wohnraumüberwachung und zur Online-Durchsuchung:
BVerfGE 141, 220 <273 f. Rn. 115>; allgemein zur Subsidiarität:
Müller/Schwabenbauer, in: Lisken/Denninger/Bäcker PolR-HdB, 8.
Aufl. 2026, Kap. 6 Rn. 237.

§ 28a Abs. 1 Satz 1 ASOG erstreckt sich von vornherein sowohl auf
Polizeipflichtige als auch auf seine Kontakt- und Begleitpersonen, ohne
insofern eine Subsidiarität anzuordnen.

(v) Kein Schutz vor Diskriminierung

Schließlich sind Regelungen zum Schutz vor Fehlern, Diskriminierung
und Datenmissbrauch erforderlich,

siehe dazu bereits oben unter I. 4. b) ee).

Da der automatisierte Datenabgleich mittels KI fehleranfällig ist und ein
Diskriminierungsrisiko birgt,

siehe oben 2.,

ist eine gesetzliche Schutzvorkehrung gegen eben solche
diskriminierenden Algorithmen notwendig, um den Vorgaben des Art. 10
VvB gerecht zu werden und eine verhältnismäßige Eingriffsgrundlage in
das Recht auf informationelle Selbstbestimmung zu stellen,

Ogorek, LTZ 2024, 274 (280).

§ 28a ASOG lässt Schutzvorkehrungen gegen Diskriminierung gänzlich vermissen. Anders als § 42d Abs. 1 Satz 2 und § 47a Abs. 1 Satz 6 ASOG enthält § 28a ASOG keine Klausel, nach der diskriminierende Algorithmen weder herausgebildet noch verwendet werden dürfen. Eine verpflichtende Testung gemäß § 42d ASOG ist nicht vorgesehen.

4. Verstoß gegen Art. 26 VvB

Da § 28a ASOG auch zur Auswertung von Fotos von Versammlungen ermächtigt,

siehe oben 3. b) aa) (ii). und bb) (ii),

liegt auch ein Eingriff in die Versammlungsfreiheit nach Art. 26 VvB vor,

BVerfG, Beschluss des Ersten Senats vom 17. Februar 2009 – 1 BvR 2492/08 –, Rn. 131.

Das Verhältnis von Versammlungsfreiheit und Recht auf informationelle Selbstbestimmung ist ungeklärt,

siehe einerseits BVerfG, Beschluss des Ersten Senats vom 17. Februar 2009 – 1 BvR 2492/08 –, Rn. 111, andererseits BVerfGE 65, 1 <43 Rn. 154>.

Sofern die Versammlungsfreiheit nicht von Art. 33 VvB verdrängt ist, ist auch dieser Eingriff unangemessen. Wer befürchten muss, im Rahmen der Teilnahme an einer Versammlung automatisiert identifiziert oder wiedererkannt zu werden, kann von der Teilnahme Abstand nehmen. Angesichts der herausragenden Bedeutung der Versammlungsfreiheit für die demokratische Willensbildung steht die mit der anlasslosen Verarbeitung von Versammlungsbildern verbundene Beeinträchtigung außer Verhältnis zu dem erzielten Sicherheitsgewinn.

IV. §§ 42a, 42b Abs. 4 Satz 1 ASOG (Zweckbindung und Kennzeichnung)

Die §§ 42a, 42b Abs. 4 Satz 1 ASOG verstoßen gegen das IT-Grundrecht aus Art. 7 i.V.m. Art. 6 VvB, das Fernmeldegeheimnis aus Art. 16 VvB, die Unverletzlichkeit der Wohnung aus Art. 28 Abs. 2 VvB sowie gegen das Recht auf informationelle Selbstbestimmung aus

Art. 33 VvB, soweit sie zu einer Weiterverarbeitung nicht gekennzeichneten Daten ermächtigen.

Die Normen regeln die Zweckbindung und Zweckänderung bei der Weiterverarbeitung personenbezogener Daten (§ 42a ASOG) sowie deren Kennzeichnung in polizeilichen Informationssystemen (§ 42b ASOG) (1.). Unter bestimmten Voraussetzungen dürfen auch nicht gekennzeichnete Daten weiterverarbeitet werden, sodass die Einhaltung des Zweckbindungsgrundsatzes in der Praxis nicht sichergestellt ist. Bis zum 1. Januar 2031 sind die Ausnahmen von der Kennzeichnungspflicht noch weiter (2.).

Die Weiterverarbeitung personenbezogener Daten greift erneut in diejenigen Grundrechte ein, in die bereits durch die ursprüngliche Datenerhebung eingegriffen wurde (3.). Diese Eingriffe sind nicht gerechtfertigt (4.). Zur Wahrung des verfassungsrechtlichen Zweckbindungsgrundsatzes ist eine wirksame Kennzeichnung der Daten erforderlich. § 42b ASOG lässt jedoch weitreichende – bis zum 1. Januar 2031 sogar noch umfassendere – Ausnahmen von der Kennzeichnungspflicht und vom Verbot der Weiterverarbeitung nicht gekennzeichneten Daten zu. Die Ausnahmeregelung ist daher unverhältnismäßig.

1. Gesetz und Gesetzesbegründung

§ 42a ASOG enthält eine Befugnis zur Weiterverarbeitung personenbezogener Daten. Während § 42a Abs. 1 ASOG die Weiterverarbeitung innerhalb der Zweckbindung regelt, enthält § 42a Abs. 2 ASOG eine Befugnis zur zweckändernden Weiterverarbeitung, die sich am Grundsatz der hypothetischen Datenneuerhebung orientiert.

Der praktischen Umsetzung dieser Vorgaben dient § 42b ASOG. Nach § 42b Abs. 1 ASOG sind personenbezogene Daten bei der Speicherung in Informationssystemen zu kennzeichnen. Nach § 42b Abs. 2 ASOG dürfen nicht gekennzeichnete Daten nicht weiterverarbeitet oder übermittelt werden. § 42b Abs. 4 Satz 1 ASOG enthält jedoch Ausnahmen. Danach entfällt die Pflicht zur Kennzeichnung und das Verbot der Weiterverarbeitung nicht gekennzeichneten Daten, soweit

eine Kennzeichnung tatsächlich nicht möglich ist, technisch nicht möglich ist oder einen unverhältnismäßigen technischen Aufwand erfordern würde.

Die Normen haben folgenden Wortlaut:

§ 42a

Zweckbindung und Grundsatz der hypothetischen Datenneuerhebung

(1) Die Ordnungsbehörden und die Polizei können personenbezogene Daten, die sie selbst erhoben haben, jeweils selbst weiterverarbeiten

1. zur Erfüllung derselben Aufgabe, der die Ermächtigungsgrundlage dient, die der Erhebung zugrunde lag,

2. zum Schutz derjenigen Rechtsgüter oder Rechte, den die der Erhebung zugrunde liegende Ermächtigungsgrundlage bezweckt, und

3. zur vorbeugenden Bekämpfung solcher Straftaten oder Ordnungswidrigkeiten, deren Verhütung die der Erhebung zugrunde liegende Ermächtigungsgrundlage bezweckt.

Das Gleiche gilt für personenbezogene Daten, die die Ordnungsbehörden und die Polizei nicht selbst erhoben haben, mit der Maßgabe, dass für die Weiterverarbeitung der Zweck der rechtmäßigen Speicherung zu berücksichtigen ist.

(2) Die Ordnungsbehörden und die Polizei können zur Erfüllung ihrer Aufgaben personenbezogene Daten zu anderen Zwecken als denjenigen, zu denen diese erhoben worden sind, weiterverarbeiten, wenn bezogen auf die Ermächtigungsgrundlage, die der Erhebung der weiterzuverarbeitenden Daten im Einzelfall zugrunde lag,

1. mindestens

a) Straftaten oder Ordnungswidrigkeiten von vergleichbarem Gewicht verhütet oder verfolgt oder

b) Rechtsgüter oder sonstige Rechte von vergleichbarer Bedeutung geschützt

werden sollen und

2. sich im Einzelfall konkrete Ermittlungsansätze zur

a) Verhütung oder Verfolgung solcher Straftaten oder Ordnungswidrigkeiten ergeben oder

b) Abwehr von in einem übersehbaren Zeitraum drohenden Gefahren für mindestens vergleichbar bedeutsame Rechtsgüter oder sonstige Rechte erkennen lassen,

soweit nicht Vorschriften dieses Gesetzes oder andere Rechtsvorschriften die zweckändernde Weiterverarbeitung besonders regeln oder eine Datenerhebung zu dem anderen Zweck mit vergleichbaren Mitteln zulassen. Abweichend von Satz 1 können die vorhandenen zur Identifizierung dienenden Daten einer Person, wie insbesondere Namen, Geschlecht, Geburtsdatum, Geburtsort,

Staatsangehörigkeit, Anschrift, auch weiterverarbeitet werden, um entsprechende Identifizierungen vorzunehmen. Die Sätze 1 und 2 gelten entsprechend für personenbezogene Daten, denen keine Erhebung vorausgegangen ist, mit der Maßgabe, dass für die Weiterverarbeitung der Zweck der Speicherung zu berücksichtigen ist. Eine Weiterverarbeitung zu anderen Zwecken liegt nicht vor, wenn sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen dient. Der Zugriff auf personenbezogene Daten ist insoweit nur zulässig, als er für die Ausübung dieser Befugnisse unverzichtbar ist. § 15 Absatz 1 Satz 1 und Absatz 5 sowie § 34 des Berliner Datenschutzgesetzes finden keine Anwendung.

(3) Die Weiterverarbeitung personenbezogener Daten nach Absatz 1 oder Absatz 2, die durch einen verdeckten Einsatz technischer Mittel in oder aus Wohnungen oder durch einen verdeckten Eingriff in informationstechnische Systeme erlangt wurden, ist zudem nur zulässig, wenn im Einzelfall die jeweilige Gefahrenschwelle im Sinne von § 25b Absatz 1 Satz 1 beziehungsweise § 26b Absatz 1 in Verbindung mit § 26a Absatz 1 erreicht ist. Erfolgt die Weiterverarbeitung nach Satz 1 zweckändernd, muss die Zweckänderung im Einzelfall festgestellt und dokumentiert werden. Bildaufnahmen oder -aufzeichnungen, die aus einer Maßnahme nach § 25b Absatz 1 erlangt wurden, dürfen nicht zu Strafverfolgungszwecken weiterverarbeitet werden.

(4) Bei der Weiterverarbeitung von personenbezogenen Daten ist durch organisatorische und technische Vorkehrungen sicherzustellen, dass die Absätze 1 bis 3 eingehalten werden.

§ 42b Kennzeichnung

(1) Bei der Speicherung in Informationssystemen sind personenbezogene Daten wie folgt zu kennzeichnen:

1. Angabe des Mittels der Erhebung einschließlich der Angabe, ob die Daten offen oder verdeckt erhoben wurden,
2. Angabe der Kategorie betroffener Personen bei denjenigen Personen, zu denen der Identifizierung dienende Daten, wie insbesondere Namen, Geschlecht, Geburtsdatum, Geburtsort, Staatsangehörigkeit, Anschrift, angelegt wurden,
3. Angabe der Rechtsgüter oder sonstigen Rechte, deren Schutz die Erhebungsvorschrift bezweckt, oder der Straftaten oder Ordnungswidrigkeiten, deren Verfolgung oder Verhütung die Erhebungsvorschrift bezweckt,
4. Angabe der Stelle, die die Daten erhoben hat.

Die Kennzeichnung nach Satz 1 Nummer 1 kann durch die Angabe der Rechtsgrundlage der jeweiligen Mittel der Datenerhebung ergänzt werden. Personenbezogene Daten, denen keine Erhebung vorausgegangen ist, sind, soweit möglich, nach Satz 1 zu kennzeichnen; darüber hinaus sind die erste diese Daten verarbeitende Stelle und, soweit möglich, diejenige Stelle, von der die Daten erlangt wurden, anzugeben. § 51a Absatz 2 bleibt unberührt.

(2) Personenbezogene Daten, die nicht nach Absatz 1 gekennzeichnet sind, dürfen nicht weiterverarbeitet oder übermittelt werden.

(3) Nach einer Übermittlung an eine andere Stelle hat diese die Kennzeichnung aufrechtzuerhalten.

(4) Die Absätze 1 bis 3 gelten nicht, soweit eine Kennzeichnung

1. tatsächlich nicht möglich ist,

2. technisch nicht möglich ist oder einen unverhältnismäßigen technischen Aufwand erfordern würde.

Auf Datenverarbeitungen nach § 42d findet dies keine Anwendung.

Ab dem 1. Januar 2031 hat § 42b Abs. 4 ASOG folgenden Wortlaut:

(4) Die Absätze 1 bis 3 gelten nicht, soweit eine Kennzeichnung tatsächlich nicht möglich ist. Auf Datenverarbeitungen nach § 42d findet dies keine Anwendung.

Die Ausnahme nach § 42b Abs. 4 Satz 1 Nr. 1 ASOG, nach der eine personenbezogene Daten nicht zu kennzeichnen sind, wenn dies tatsächlich nicht möglich ist, gilt unbefristet. Sie kann etwa dadurch gegeben sein, dass nicht bekannt oder nicht feststellbar ist, wer die Daten erhoben hat oder zu welchem Zweck diese ursprünglich erhoben wurden. Bis zum 1. Januar 2031 gilt zudem die Ausnahme von der Kennzeichnungspflicht, wenn dies technisch nicht möglich ist oder einen unverhältnismäßigen Aufwand erfordern würde (§ 42b Abs. 4 Satz 1 Nr. 2 ASOG). Ausweislich der Begründung wurde die Frist sowohl als erforderlich als auch als ausreichend angesehen, um der Polizei Berlin die Umsetzung der Kennzeichnungspflicht in ihren Informationssystemen zu ermöglichen,

Abgh-Drs. 19/2553, S. 281.

Das Verbot der Weiterverarbeitung nicht gekennzeichneten Daten in § 42b Abs. 2 ASOG wurde erst durch einen Änderungsantrag aufgenommen. Die Ausnahme in § 42b Abs. 4 Satz 1 ASOG wurde ausdrücklich auf dieses Verbot erstreckt. Laut der Begründung ginge ein absolutes Verbot der Weiterverarbeitung nicht gekennzeichneten Daten zu weit, „da es die – der Abwehr von Gefahren dienende! – Polizeiarbeit in einem nicht mehr hinnehmbaren Maß erheblich einschränken würde“,

Änderungsantrag der Fraktion der CDU und der Fraktion der SPD zur Drucksache 19/2553, **Anlage 6**, S. 36.

2. Anwendungsszenarien

Bis zum 1. Januar 2031 dürfen nicht gekennzeichnete Daten weiterverarbeitet werden, solange eine Kennzeichnung technisch noch nicht möglich oder mit unverhältnismäßigem Aufwand verbunden ist. Zwar gelten die Grundsätze der Zweckbindung nach § 42a ASOG, jedoch ist ihre Einhaltung bei nicht gekennzeichneten Daten praktisch unmöglich.

So ist es beispielsweise möglich, dass Daten aus einer Wohnraumüberwachung in Informationssystemen der Polizei gespeichert sind, ohne dass dies gekennzeichnet ist. Zwar enthält § 42a Abs. 3 ASOG für diesen Fall strenge Vorgaben für die Weiterverarbeitung. Die Einhaltung dieser Vorgaben ist jedoch praktisch nicht möglich, da die Person, die die Daten weiterverarbeitet, nicht erkennen kann, dass sie aus einer Wohnraumüberwachung stammen.

3. Eingriffe in die Schutzbereiche von Grundrechten

Die Weiterverarbeitung von personenbezogenen Daten nach § 42a ASOG greift in das IT-Grundrecht aus Art. 7 VvB i.V.m. Art. 6 Satz 1 VvB, das Fernmeldegeheimnis aus Art. 16 VvB, die Unverletzlichkeit der Wohnung nach Art. 28 Abs. 2 VvB und das Recht auf informationelle Selbstbestimmung aus Art. 33 VvB ein.

Die Ermächtigung zu Weiterverarbeitung von Daten begründet einen neuen Eingriff in das Grundrecht, in das durch die Datenerhebung eingegriffen wurde. Die Weiterverarbeitung ist an den Grundrechten zu messen, die für die Datenerhebung maßgeblich waren,

BVerfGE 141, 220 <324 ff. Rn. 275 ff.>.

§ 42a ASOG ermächtigt zur Weiterverarbeitung von personenbezogenen Daten, die die Ordnungsbehörden und die Polizei selbst erhoben haben. Diese Daten können durch verschiedene polizeiliche Maßnahmen erhoben worden sein. Es können unter anderem Daten weiterverarbeitet werden, die durch eine Telekommunikationsüberwachung (§ 26 ASOG, Eingriff in Art. 16 VvB), durch eine Quellen-Telekommunikationsüberwachung oder Online-Durchsuchung (§§ 26a, 26b ASOG, Eingriffe in das IT-Grundrecht aus Art. 7 VvB i.V.m. Art. 6 Satz 1 VvB und Art. 16 VvB) sowie durch eine

Wohnraumüberwachung oder Wohnungsdurchsuchung (§§ 25b, § 36 ASOG, Eingriffe in Art. 28 Abs. 2 Satz 1 VvB) erhoben wurden. Im Übrigen handelt es sich jedenfalls um Daten, die unter Eingriff in das Recht aus Art. 33 VvB erhoben wurden.

Die Weiterverarbeitung greift somit in diese Grundrechte ein.

4. Keine Rechtfertigung

Diese Eingriffe sind nicht gerechtfertigt. Die Rechtfertigung der Weiterverarbeitung richtet sich nach den Grundsätzen der Zweckbindung und Zweckänderung,

BVerfGE 141, 220 <324 ff. Rn. 275 ff.>.

Zur Wahrung der verfassungsrechtlichen Anforderungen der Zweckbindung müssen hinreichend normenklare Regelungen getroffen sein, die die Einhaltung des Grundsatzes der Zweckbindung rechtlich und praktisch sichern. Praktisch ist zur Einhaltung des verfassungsrechtlichen Zweckbindungsgrundsatzes insbesondere eine Kennzeichnung von Daten erforderlich,

vgl. BVerfG, Urteil des Ersten Senats vom 16. Februar 2023 – 1 BvR 1547/19 –, Rn. 65.

Der Grundsatz der hypothetischen Datenneuerhebung lässt sich in sicherheitsbehördlichen Dateien nur umsetzen, wenn die darin gespeicherten personenbezogenen Daten mit den relevanten Zusatzinformationen versehen, das heißt gekennzeichnet sind,

Weichert, NVwZ 2022, 844 (845).

Ausnahmen von der Kennzeichnungspflicht können zwar für einen Übergangszeitraum hingenommen werden. Dann muss jedoch sichergestellt sein, dass die nicht gekennzeichneten Daten nicht weiterverarbeitet werden. Solange die Berliner Polizei die technischen Voraussetzungen zur Kennzeichnung nicht schafft, kann sie das Instrument der hypothetischen Datenneuerhebung nicht gemäß den Vorgaben des Bundesverfassungsgerichts in der Breite anwenden,

Berliner Beauftragte für Datenschutz und Informationsfreiheit, Stellungnahme zum Gesetzentwurf zur Reform des Berliner Polizei-

und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 2**, S. 20.

§ 42b ASOG genügt diesen Anforderungen nicht. Zwar sind nach § 42b Abs. 1 ASOG die Daten zu kennzeichnen und nach § 42b Abs. 2 ASOG dürfen nicht gekennzeichnete Daten nicht weiterverarbeitet werden. § 42b Abs. 4 enthält jedoch weitreichende – bis zum 1. Januar 2031 sogar noch umfassendere – Ausnahmen nicht nur von der Kennzeichnungspflicht, sondern auch vom Weiterverarbeitungsverbot nicht gekennzeichneter Daten,

kritisch auch Botta, Stellungnahme zum Gesetz zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 3**, S. 12.

Anders als § 14 Abs. 2 BKAG enthält § 42b ASOG kein absolutes Verbot der Weiterverarbeitung und Übermittlung nicht gekennzeichneter Daten. Ein Verbot gilt nach § 42b Abs. 4 Satz 2 ASOG allein für die Datenverarbeitung im Rahmen des KI-Trainings nach § 42d ASOG.

Die Übergangsregelung beschränkt sich damit nicht auf ein bloß technisches Defizit bei der Umsetzung der Kennzeichnungspflicht, sondern ermöglicht eine Datenverarbeitung, bei der die maßgeblichen rechtlichen Grenzen der Verwendung der Daten gerade nicht mehr bestimmt werden können. Damit betrifft die Übergangsregelung zugleich eine grundlegende Voraussetzung für eine verfassungsgemäße Datenverarbeitung. Die nach den verfassungsgerichtlichen Maßstäben erforderliche Differenzierung nach Datenarten und ihrer jeweiligen Eingriffsintensität setzt voraus, dass die Herkunft und Kategorie eines Datensatzes zuverlässig bestimmbar ist. Erst hierdurch lassen sich die für seine weitere Verwendung geltenden Schwellen bestimmen. Sind die Daten hingegen nicht kategorisiert, kann nicht mehr festgestellt werden, welcher rechtliche Maßstab für ihre Verwendung gilt. Die Schwellen für die Weiterverwendung werden dadurch nicht lediglich erschwert anwendbar, sondern faktisch ausgehebelt.

Das ist nicht verhältnismäßig. Die nachträgliche Kennzeichnung mag im Einzelfall zu einer gewissen Verzögerung der Datenweiterverarbeitung führen. Diese Verzögerung liegt jedoch in der Verantwortungssphäre

der Polizei. Angesichts der ansonsten drohenden potentiell schwerwiegenden Verletzung des Zweckbindungsgrundsatzes ist eine solche Verzögerung hinzunehmen,

im Ergebnis ebenso Berliner Beauftragte für Datenschutz und Informationsfreiheit, Stellungnahme zum Gesetzentwurf zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 2**, S. 20.

V. § 42d ASOG (Training und Testung von KI-Systemen)

§ 42d ASOG verstößt gegen das IT-Grundrecht aus Art. 7 VvB i.V.m. Art. 6 Satz 1 VvB, das Fernmeldegeheimnis aus Art. 16 VvB, die Unverletzlichkeit der Wohnung aus Art. 28 Abs. 2 VvB sowie gegen das Recht auf informationelle Selbstbestimmung aus Art. 33 VvB.

Die Norm schafft eine Rechtsgrundlage für die Weiterverarbeitung rechtmäßig erhobener personenbezogener Daten zum Training und zur Testung von KI-Systemen (1.). Hierfür können unter bestimmten Voraussetzungen auch nicht anonymisierte personenbezogene Daten weiterverarbeitet und an Auftragsverarbeitende oder sonstige Dritte übermittelt werden (2.).

Die zweckändernde Weiterverarbeitung personenbezogener Daten zum Training und zur Testung von KI-Systemen greift erneut in diejenigen Grundrechte ein, in die bereits durch die ursprüngliche Datenerhebung eingegriffen wurde (3.). Diese Eingriffe sind nicht gerechtfertigt (4.). § 42d ASOG durchbricht den Grundsatz der hypothetischen Datenneuerhebung (4. a)). Angesichts des hohen Eingriffsgewichts der Datenweiterverarbeitung (4. b) aa)) genügen die gesetzlichen Voraussetzungen den verfassungsrechtlichen Anforderungen nicht (4. b) bb)). Zudem enthält die Norm keine hinreichenden Schutzvorkehrungen (4. b) cc)) und ermöglicht eine unverhältnismäßig weitgehende Weitergabe personenbezogener Daten an Auftragsverarbeitende und sonstige Dritte (4. b) dd)).

1. Gesetz und Gesetzesbegründung

Der neu eingefügte § 42d ASOG schafft eine Rechtsgrundlage für das Training und die Testung von KI-Systemen mit zu anderen Zwecken

rechtmäßig erhobenen personenbezogenen Daten. Kann der Zweck des Tests oder Trainings mit anonymisierten oder pseudonymisierten Daten nicht erreicht werden oder sind die Daten nur mit unverhältnismäßigem Aufwand zu anonymisieren, können auch personenbezogene Daten verwendet werden (§ 42d Abs. 2 ASOG). Wenn die Verarbeitung durch Polizei und Feuerwehr auch unter Zuhilfenahme Auftragsverarbeitender nur mit unverhältnismäßigem Aufwand möglich ist, dürfen personenbezogene Daten auch an Dritte weitergegeben werden, um KI-Systeme zu trainieren und zu testen (§ 42d Abs. 3 ASOG). Verwaltungsvorschriften sollen die Anforderungen des § 42d Abs. 1 bis 3 ASOG konkretisieren.

Die Norm hat folgenden Wortlaut:

§ 42d
Training und Testung von KI-Systemen

(1) Polizei und Feuerwehr können die bei ihnen jeweils rechtmäßig gespeicherten personenbezogenen Daten auch über die vorgesehene Speicherdauer hinaus weiterverarbeiten, wenn dies erforderlich ist, um KI-Systeme, die der Erfüllung ihrer jeweiligen Aufgaben dienen, unter Verwendung dieser Daten zu trainieren und zu testen. Bei der Weiterverarbeitung ist sicherzustellen, dass diskriminierende Algorithmen weder herausgebildet noch verwendet werden. Soweit wie technisch möglich, muss die Nachvollziehbarkeit des verwendeten Verfahrens sichergestellt werden. Die Weiterverarbeitung von personenbezogenen Daten, die aus in § 42c Absatz 2 genannten Maßnahmen erlangt wurden, ist unzulässig. Personenbezogene Daten nach Satz 1 dürfen nicht zum Trainieren oder Testen von KI-Systemen weiterverarbeitet werden, wenn die Daten nicht mit Hilfe solcher KI-Systeme erhoben oder verarbeitet werden dürften.

(2) Personenbezogene Daten sind für die Verwendung zu Test- oder Trainingszwecken zu anonymisieren. Kann der Zweck des Tests oder Trainings mit anonymisierten Daten nicht erreicht werden oder ist die Anonymisierung nur mit unverhältnismäßigem Aufwand möglich, sind sie zu pseudonymisieren. Kann der Zweck des Tests oder Trainings auch mit pseudonymisierten Daten nicht erreicht werden oder ist auch die Pseudonymisierung nur mit unverhältnismäßigem Aufwand möglich, dürfen personenbezogene Daten verwendet werden. Besondere Kategorien personenbezogener Daten dürfen nur unter Gewährleistung von Garantien im Sinne des § 51a Absatz 2 verwendet werden. Die Daten sind unverzüglich zu löschen oder unumkehrbar zu anonymisieren, sobald sie zu Test- oder Trainingszwecken nicht mehr benötigt werden, sonst spätestens nach zwei Jahren, es sei denn, ihre Weiterverarbeitung ist nach anderen Rechtsvorschriften zulässig. Die Löschung ist zu protokollieren. Es ist unzulässig,

1. aus den nach Absatz 1 trainierten oder getesteten KI-Systemen die ursprünglichen personenbezogenen Daten wiederherzustellen,
2. personenbezogene Daten, die gemäß Satz 1 anonymisiert wurden, zu de-anonymisieren.

(3) Zur Durchführung von Maßnahmen nach Absatz 1 und nach Maßgabe von Absatz 2 dürfen Polizei und Feuerwehr personenbezogene Daten an Auftragsverarbeitende weitergeben, wenn eine Verarbeitung durch sie selbst nicht oder nur mit unverhältnismäßigem Aufwand möglich ist. Ist die Verarbeitung durch Polizei und Feuerwehr auch unter Zuhilfenahme Auftragsverarbeitender nicht oder nur mit unverhältnismäßigem Aufwand möglich, dürfen Polizei und Feuerwehr personenbezogene Daten auch an Dritte zu dem in Satz 1 genannten Zweck übermitteln. Auftragsverarbeitende oder zur Verarbeitung eingesetzte Dritte müssen ihren Sitz in einem Mitgliedstaat der Europäischen Union oder in einem Schengen-assoziierten Staat haben; die Daten dürfen nur dorthin weitergeleitet und nur dort weiterverarbeitet werden. § 42c Absatz 3, 4 und 5 Satz 1 gilt entsprechend. Die bei Auftragsverarbeitenden oder zur Verarbeitung eingesetzten Dritten eingesetzten Personen sind nach § 1 des Verpflichtungsgesetzes zu verpflichten, sofern dies geboten erscheint. Die Übermittlung von Daten nach Absatz 1 Satz 4 ist unzulässig. Auftragsverarbeitende und zur Verarbeitung eingesetzte Dritte dürfen die übermittelten Daten nur im Rahmen des jeweiligen Trainings und der jeweiligen Tests verarbeiten. Sie dürfen die trainierten Modelle für eigene Zwecke weiternutzen, wenn Polizei oder Feuerwehr dem zugestimmt haben und sichergestellt werden kann, dass aus den trainierten Modellen keine Trainingsdaten abgeleitet werden können.

(4) Verwaltungsvorschriften bestimmen das Nähere insbesondere zu

1. dem technische Verfahren nach Absatz 1,
2. der Art und dem Umfang der zu verarbeitenden Daten,
3. dem Personenkreis, der von der Verarbeitung betroffen ist,
4. den Sicherungsmaßnahmen zur Datenaktualität und -qualität,
5. den Sicherungsmaßnahmen zur Verhinderung unbefugter Datenzugriffe,
6. den Mindeststandards zur technischen Durchführung der Anonymisierung und Pseudonymisierung von Daten,
7. der Beschreibung eines etwaigen unverhältnismäßigen Aufwands im Sinne von Absatz 2 Satz 2 und 3 und
8. den Lösch- und Protokollierungspflichten.

Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit ist vor Erlass oder einer Änderung der Verwaltungsvorschriften anzuhören. Die Verwaltungsvorschriften sind zu veröffentlichen.

Nach der Gesetzesbegründung soll mit § 42d ASOG eine spezifische Rechtsgrundlage für die Verwendung von Echtdaten für das Training und die Testung von KI-Systemen geschaffen werden. Zum Begriff des KI-Systems verweist die Gesetzesbegründung auf Art. 3 Nr. 1 KI-Verordnung. § 42d Abs. 1 Satz 4 ASOG nehme personenbezogene Daten, die durch die in § 42c Abs. 2 ASOG genannten, besonders tief in die Privat- bzw. Intimsphäre einer Person eingreifenden polizeilichen Maßnahmen erhoben wurden, von der Weiterverarbeitung zum Zwecke

des Trainings oder der Testung von KI-Systemen aus. § 42d Abs. 2 ASOG sehe ein abgestuftes Konzept vor. § 42d Abs. 3 ASOG regele das Training und die Testung von KI-Systemen im Wege der Auftragsverarbeitung und durch Dritte,

Abgh-Drs. 19/2553, S. 287 ff.

Im Laufe des Gesetzgebungsverfahrens wurden geringfügige Änderungen vorgenommen,

Änderungsantrag der Fraktion der CDU und der Fraktion der SPD zur Drucksache 19/2553, **Anlage 6**, S. 13 und 37.

2. Anwendungsszenarien

Weder § 42d ASOG noch die Gesetzesbegründung enthalten Angaben dazu, wie konkret die neue Befugnis zum Einsatz kommen soll. Da § 42d ASOG grundsätzlich alle denkbaren KI-Systeme erfasst, sind verschiedene Einsatzszenarien denkbar.

Die Befugnis betrifft somit nicht nur KI-Systeme, deren Verwendung im ASOG explizit vorgesehen ist,

z.B. § 24e Abs. 4, § 28a oder § 47a ASOG, siehe dazu oben I. und III. und unten VI.,

sondern auch solche KI-Systeme, deren Nutzung auf andere Rechtsgrundlagen, wie zum Beispiel die Datenverarbeitungsgeneralklausel nach § 42 ASOG, gestützt wird.

Vergleichbare Regelungen gibt es bisher z.B. in § 37a des Gesetzes über die Datenverarbeitung der Polizei Hamburg und § 57a Polizeigesetz des Landes Baden-Württemberg.

In Hamburg soll die entsprechende Norm dazu dienen, die Videoüberwachung auszubauen und zu automatisieren,

vgl. netzpolitik.org vom 14. Januar 2025, Hamburger Polizei soll KI mit personenbezogenen Daten trainieren, <https://netzpolitik.org/2025/videoeueberwachung-hamburger-polizei-soll-ki-mit-personenbezogenen-daten-trainieren/>; NDR vom 31. Juli 2025, Hamburger Polizei will KI mit Videos von Passanten trainieren, <https://www.ndr.de/nachrichten/hamburg/polizei-hamburg-will-ki-mit-videos-von-passantentrainieren,kameraueberwachung-102.html>.

3. Eingriffe in die Schutzbereiche von Grundrechten

Die Nutzung von rechtmäßig erhobenen personenbezogenen Daten für das Training und den Test von KI-Systemen greift in das IT-Grundrecht aus Art. 7 VvB i.V.m. Art. 6 Satz 1 VvB, das Fernmeldegeheimnis aus Art. 16 VvB, die Unverletzlichkeit der Wohnung nach Art. 28 Abs. 2 VvB und das Recht auf informationelle Selbstbestimmung aus Art. 33 VvB ein.

§ 42d ASOG ermächtigt zur zweckändernden Weiterverarbeitung von rechtmäßig gespeicherten personenbezogenen Daten zu anderen Zwecken,

vgl. dazu bereits oben unter IV. 3.

Die Weiterverarbeitung zum Training und zur Testung von KI-Systemen stellt eine Zweckänderung dar, da die Erhebungsbefugnisse keinen derartigen Zweck kennen.

Diese Daten können durch verschiedene polizeiliche Maßnahmen erhoben worden sein. Ausgenommen sind nach § 42d Abs. 1 Satz 4 ASOG nur Daten, die aus einer Maßnahme nach § 42c Abs. 2 ASOG erlangt wurden.

Für das Training und die Testung von KI-Systemen können daher unter anderem Daten verwendet werden, die durch eine Telekommunikationsüberwachung (§ 26 ASOG, Eingriff in Art. 16 VvB), eine Quellen-Telekommunikationsüberwachung (§ 26a ASOG, Eingriff in das IT-Grundrecht aus Art. 7 VvB i.V.m. Art. 6 Satz 1 VvB und Art. 16 VvB) oder durch eine Wohnungsdurchsuchung (§ 36 ASOG, Eingriff in Art. 28 Abs. 2 Satz 1 VvB) erhoben worden sind. Im Übrigen handelt es sich jedenfalls um Daten, die unter Eingriff in das Recht aus Art. 33 VvB erhoben worden sind.

4. Keine Rechtfertigung

Die mit der Nutzung von rechtmäßig erhobenen personenbezogenen Daten für das Training und den Test von KI-Systemen verbundenen Eingriffe sind verfassungsrechtlich nicht gerechtfertigt.

§ 42d ASOG durchbricht den Grundsatz der hypothetischen Datenneuerhebung (a)). Diese Durchbrechung ist unverhältnismäßig (b)).

a) Durchbrechung des Grundsatzes der hypothetischen Datenneuerhebung

Aus den Grundsätzen der Zweckbindung und Zweckänderung folgt, dass sich die Eingriffsschwellen an denen orientieren, die für die Datenerhebung bestehen. Informationen, die durch besonders eingriffsintensive Maßnahmen erlangt wurden, können auch nur zu besonders gewichtigen Zwecken genutzt werden. Es gilt das Kriterium der hypothetischen Datenneuerhebung,

vgl. BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, Rn. 286 f.

Das Kriterium der hypothetischen Datenneuerhebung gilt allerdings nicht schematisch abschließend und schließt die Berücksichtigung weiterer Gesichtspunkte nicht aus. Das Erfordernis einer Gleichgewichtigkeit der neuen Nutzung bleibt hierdurch jedoch unberührt,

BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, Rn. 287.

Voraussetzung für eine Zweckänderung ist jedenfalls, dass die neue Nutzung der Daten dem Schutz von Rechtsgütern oder der Aufdeckung von Straftaten eines solchen Gewichts dient, die verfassungsrechtlich ihre Neuerhebung mit vergleichbar schwerwiegenden Mitteln rechtfertigen könnten,

BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, Rn. 288.

Nicht in jedem Fall identisch sind die Voraussetzungen einer Zweckänderung mit denen einer Datenerhebung hingegen hinsichtlich des erforderlichen Konkretisierungsgrades der Gefahrenlage oder des Tatverdachts. Als neu zu rechtfertigender Eingriff bedarf aber auch die Ermächtigung zu einer Nutzung für andere Zwecke eines eigenen, hinreichend spezifischen Anlasses. Verfassungsrechtlich geboten, aber regelmäßig auch ausreichend, ist insoweit, dass sich aus den Daten – sei es aus ihnen selbst, sei es in Verbindung mit weiteren Kenntnissen der Behörde – ein konkreter Ermittlungsansatz ergibt,

Diese Grundsätze, die in § 42a Abs. 2 ASOG umgesetzt sind, werden durch § 42d ASOG durchbrochen. § 42d ASOG dient weder unmittelbar der Verhütung oder Verfolgung von vergleichbar schwerwiegenden Straftaten oder dem Schutz von vergleichbar bedeutenden Rechtsgütern noch setzt die Vorschrift einen Ermittlungsansatz voraus. § 42d ASOG ist vielmehr eine Rechtsvorschrift, die die zweckändernde Weiterverarbeitung besonders regelt (§ 42a Abs. 2 Satz 1 ASOG a.E.).

b) Unverhältnismäßigkeit

Unter bestimmten, engen Voraussetzungen kann eine zweckändernde Datenweiterverarbeitung auch unterhalb dieser Schwelle zugelassen werden.

So ist anerkannt, dass die zweckändernde Datenweiterverarbeitung zu Forschungszwecken, archivarischen und statistischen Zwecken sowie zur Aus- und Fortbildung unter anderen Voraussetzungen gerechtfertigt werden kann (vgl. § 42c ASOG).

Gerechtfertigt wird dies damit, dass bei diesen Sekundärnutzungen eine operative Nutzung für polizeiliche Zwecke zukünftig weitestgehend auszuschließen sei. Die Regelungen zielten gerade nicht auf die Nutzung zur Gefahrenabwehr oder Strafverfolgung ab, sodass sich eine gesetzgeberische Entscheidung zur Privilegierung dieser Weiterverarbeitungszwecke unter Berücksichtigung der dort näher geregelten technisch-organisatorischen Maßnahmen und Garantien rechtfertigen lasse,

Pohl-Schönmehl, in: BeckOK SicherheitsR/PolR Bund, 3. Edition 2026, BKAG § 12 Rn. 18; siehe auch Weichert NVwZ 2022, 844 (848)).

Auch für das Training und die Testung von polizeilichen KI-Systemen ist eine Privilegierung grundsätzlich denkbar. Erforderlich hierfür sind jedoch hinreichend bestimmte Regelungen, die das Eingriffsgewicht der Datenweiterverarbeitung ins Verhältnis zu dem damit verfolgten Zweck setzen und Vorkehrungen zum Schutz der Daten treffen. Solche Regelungen liegen nicht vor.

Die angegriffene Vorschrift ermächtigt zu Datenweiterverarbeitungen mit potenziell hohem Eingriffsgewicht (aa)), ohne sie auf hinreichend gewichtige Anlässe zu beschränken (bb)). Zudem sind die Vorkehrungen zum Schutz personenbezogener Daten unzureichend (cc)) und die Befugnis zur Datenübermittlung ist zu weit gefasst (dd)).

aa) Eingriffsintensität

Eine zweckändernde Datenweiterverwendung kann schwer schwiegen,

vgl. Verfassungsgerichtshof des Landes Berlin, Beschluss vom 28. Mai 2004 – 81/02 –, Rn. 26.

Das Eingriffsgewicht einer zweckändernden Datenweiterverwendung richtet sich grundsätzlich nach dem Gewicht des Eingriffs der Datenerhebung,

BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19 –, Rn. 61

Die Eingriffsintensität lässt sich jedoch nicht allein mit Blick auf das Gewicht der ursprünglichen Datenerhebung beurteilen. Es müssen auch spezifische, der nachfolgenden Verwendung anhaftenden Umstände berücksichtigt werden,

vgl. BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19 –, Rn. 66.

Konkrete verfassungsrechtliche Maßstäbe dafür, an welchen Kriterien das Eingriffsgewicht für die Nutzung von personenbezogenen Daten für das Training und die Testung von KI-Systemen zu bestimmen ist, bestehen noch nicht. Jedoch können auch hier die Kriterien des Bundesverfassungsgerichts zur automatisierten Datenanalyse,

siehe oben I. 4. a) bb) (i),

herangezogen werden,

Gesellschaft für Freiheitsrechte, Stellungnahme zu den Referentenentwürfen des Bundesministeriums des Inneren „Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit“ und „Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse zur Abwehr von Gefahren des internationalen Terrorismus“, 9. April 2026, <https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/stellungnahmen/OESI3/ermittlungsbefugnisse-interrorismus/gesellschaft-freiheitsrechte.pdf>, S. 22 ff.

Gemessen an diesen Maßstäben kann der mit § 42d ASOG verbundene Eingriff potenziell schwer wiegen,

vgl. Wittmann, BT-Ausschussdrucksache 20(4)493 A neu, S. 124.

Jedenfalls ist er so gewichtig, dass eine Durchbrechung des Zweckbindungsgrundsatzes nur unter strengen Voraussetzungen gerechtfertigt werden kann,

zu diesen Anforderungen unten bb).

Ausgangspunkt ist das Eingriffsgewicht der Datenerhebung. Die Daten können mit sehr eingriffsintensiven Mitteln erhoben worden sein, wie zum Beispiel durch den verdeckten Einsatz technischer Mittel außerhalb von Wohnungen (§ 25a ASOG), (Quellen-)Telekommunikationsüberwachung (§§ 26, 26a ASOG) oder Funkzellenabfragen (§ 26e ASOG).

Zudem ist der Umfang der personenbezogenen Daten, die genutzt werden können, durch § 42d ASOG kaum begrenzt. Als Datenquelle für Training und Testung von KI-Systemen kann grundsätzlich der gesamte rechtmäßig erhobene polizeiliche Datenbestand genutzt werden, inklusive Daten von Zeuginnen und Zeugen, Opfern oder Unbeteiligten,

vgl. Berliner Beauftragte für Datenschutz und Informationsfreiheit, Stellungnahme zum Gesetzentwurf zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 2**, S. 20.

§ 42d ASOG gestattet die Weiterverarbeitung von Daten eines unüberschaubaren Kreises von Personen, ohne dass das Training oder der Test mit deren Verhalten in Beziehung gebracht werden könnte oder durch das Verhalten dieser Personen veranlasst wäre. Auch die Daten unbeteiligter Dritter können für Training und Test des KI-Systems genutzt werden,

Weizenbaum-Institut, Stellungnahme zur Novellierung des Allgemeinen Sicherheits- und Ordnungsgesetzes Berlin (ASOG Bln), Policy Paper #19, März 2026, S. 22.

Auch die Art der personenbezogenen Daten, die verwendet werden können, ist kaum eingeschränkt. § 42d ASOG ermöglicht das Training

und den Test von KI-Systemen mit sensiblen personenbezogenen Daten,

vgl. Botta, Stellungnahme zum Gesetz zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 3**, S. 8.

Hierzu gehören unter anderem die besonderen Kategorien personenbezogener Daten im Sinne des § 31 Nr. 14 BInDSG. Dies sind:

- Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen,
- genetische Daten,
- biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person,
- Gesundheitsdaten und
- Daten zum Sexualleben oder zur sexuellen Orientierung.

§ 42d ASOG lässt auch zu, sämtliche denkbaren Dateiformate zu verwenden. So können auch Bilder, Videos, Audioaufnahmen genutzt werden.

Unklar ist, welche Auswirkungen die Begrenzung des § 42d Abs. 1 Satz 5 ASOG hat. Danach dürfen personenbezogene Daten nicht zum Trainieren oder Testen von KI-Systemen weiterverarbeitet werden, wenn die Daten nicht mit Hilfe solcher KI-Systeme erhoben oder verarbeitet werden dürften. Der Satz wurde durch einen Änderungsantrag eingefügt. In der Begründung wird lediglich klargestellt, dass auf die beabsichtigte Funktion des KI-Systems zur Durchführung einer bestimmten Maßnahme abzustellen ist, nicht auf den noch untrainierten Zustand,

Änderungsantrag der Fraktion der CDU und der Fraktion der SPD zur Drucksache 19/2553, **Anlage 6**, S. 37.

Da aber die möglichen Verwendungen des KI-Trainings noch nicht feststehen,

siehe oben 2.,

kann auch nicht mit hinreichender Bestimmtheit beurteilt werden, welche Auswirkungen § 42 Abs. 1 Satz 5 ASOG auf die Datenarten hat.

Die Eingriffsintensität steigt auch dadurch, dass die Speicherdauer für einmal rechtmäßig erhobene Daten so lange verlängert werden kann, wie die Daten für das Training und die Testung von KI-Systemen benötigt werden,

vgl. Abgh-Drs. 19/2553, S. 288; Berliner Beauftragte für Datenschutz und Informationsfreiheit, Stellungnahme zum Gesetzentwurf zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 2**, S. 21.

Die Löschung hat unabhängig davon erst zwei Jahre nach der Erhebung der Daten zu erfolgen (§ 42d Abs. 2 Satz 5 ASOG). Abgesehen davon ist unklar, ob eine Löschung technisch überhaupt möglich ist. So besteht etwa die Gefahr, dass KI-Systeme Trainingsdaten bei der Nutzung oder schon beim Testen des Systems ausgeben,

Kühne/Golla/Schäfer, GSZ 2025, 272 (278) mit Verweis auf Nasr/Carlini/Hayase/Jagielski/Cooper/Ippolito/Choquette-Choo/Wallace/Tramèr/Lee, Scalable Extraction of Training Data from (Production) Language Models, 2023, <https://doi.org/10.48550/arXiv.2311.17035>; Muttach/Link, CR 2023, 725 Rn. 17; Berliner Beauftragte für Datenschutz und Informationsfreiheit, Stellungnahme zum Gesetzentwurf zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 2**, S. 21.

So heißt es in einer Stellungnahme des Europäischen Datenschutzausschusses (EDSA):

„Nach Ansicht des EDSA kann es, selbst wenn ein KI-Modell nicht absichtlich darauf ausgelegt wurde, Informationen aus den Trainingsdaten auszugeben, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, doch vorkommen, dass Daten aus dem Trainingsdatensatz – einschließlich personenbezogener Daten – nach wie vor in den Parametern des Modells „absorbiert“ (d. h. durch mathematische Objekte repräsentiert) sind. Es mag sein, dass diese Daten sich von den ursprünglichen Trainingsdatenpunkten unterscheiden, aber dennoch weiterhin die ursprünglichen Informationen dieser Daten enthalten, die dann möglicherweise letztendlich direkt oder indirekt aus dem Modell entnommen oder in sonstiger Weise daraus erlangt werden

können. Soweit es möglich ist, mit Mitteln, die nach allgemeinem Ermessen wahrscheinlich genutzt werden, aus einem KI-Modell Informationen zu erlangen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, deren personenbezogene Daten für das Training eines Modells verwendet wurden, lässt dies den Schluss zu, dass ein derartiges Modell nicht anonym ist.“

EDSA, Stellungnahme 28/2024 zu gewissen Datenschutzaspekten der Verarbeitung personenbezogener Daten im Zusammenhang mit KI-Modellen, 2024, S. 15 f., Rn. 31.

Neben Art und Umfang der Daten, die für das Training und den Test von KI-Systemen genutzt werden können, kommt eingriffsverstärkend hinzu, dass die Daten grundsätzlich für das Training und den Test jeder denkbaren KI-Anwendung genutzt werden können. Welche Zweckbestimmung oder Funktionsweise das zu trainierende bzw. zu testende KI-System haben soll, schreibt § 42d ASOG nicht vor,

vgl. Berliner Beauftragte für Datenschutz und Informationsfreiheit, Stellungnahme zum Gesetzentwurf zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 2**, S. 22; Botta, Stellungnahme zum Gesetz zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 3**, S. 7.

Denkbar ist, dass auf der Grundlage von § 42d ASOG ein KI-System zur Erstellung von Bewegungs-, Verhaltens- oder Persönlichkeitsprofilen trainiert und getestet wird,

vgl. Abgh, Plenarprotokoll 19/69 vom 10. Juli 2025, S. 14.

Anders als bei der Datenweiterverwendung nach § 42c ASOG ist auch nicht ausgeschlossen, dass die Trainings- und Testdaten später operativ für polizeiliche Zwecke genutzt werden. Denn die KI-Systeme dienen der Aufgabenerfüllung der Polizei und die Trainingsdaten beeinflussen die Funktionsweise der Algorithmen. Es besteht insbesondere die Gefahr, dass das KI-System Trainingsdaten „wiedererkennt“ und Personen dadurch zu Unrecht zum Ziel von Folgemaßnahmen werden.

Das Eingriffsgewicht wird auch nicht maßgeblich durch das gestufte Schutzkonzept des § 42d Abs. 2 ASOG verringert. Danach sind

personenbezogenen Daten für die Verwendung zu Test- oder Trainingszwecken grundsätzlich zu anonymisieren. Kann der Zweck des Tests oder Trainings mit anonymisierten Daten nicht erreicht werden oder ist die Anonymisierung nur mit unverhältnismäßigem Aufwand möglich, sind die Daten zu pseudonymisieren (§ 42d Abs. 2 Satz 2 ASOG). Wenn auch eine Pseudonymisierung wegen des Zwecks des Tests oder Trainings nicht in Betracht kommt oder nur mit unverhältnismäßigem Aufwand möglich ist, dürfen auch personenbezogene Daten verwendet werden (§ 42d Abs. 2 Satz 3 ASOG). Die Möglichkeit, bei „unverhältnismäßigem Aufwand“ auch personenbezogene Daten zu verwenden, ermöglicht es, aufgrund rein wirtschaftlicher Erwägungen vom Grundsatz der Anonymisierung abzuweichen. So sieht die Gesetzesbegründung gerade vor, dass der Aufwand der Anonymisierung bzw. Pseudonymisierung unverhältnismäßig ist, wenn der Zeit- und Kostenaufwand für die Anonymisierung oder Pseudonymisierung außer Verhältnis steht zu der Zeit- und Kostenersparnis, die durch eine spätere Nutzung des KI-Systems herbeigeführt werden kann,

siehe Abgh-Drs. 19/2553, S. 288; zur Kritik daran siehe unten cc).

Hinzu kommt, dass in der Praxis eine wirksame Anonymisierung komplexer Datensätze, insbesondere bei biometrischen Daten oder Verhaltensdaten regelmäßig sehr aufwändig bis unmöglich ist. Anonymisierte Daten bergen zudem das Risiko, dass im Zuge des Anonymisierungsprozesses Details verloren gehen und Fakten verzerrt werden, die für das Training und Tests relevant sind. Die Regelung läuft daher auf eine systematische Verwendung von Echtdaten hinaus,

Berliner Beauftragte für Datenschutz und Informationsfreiheit, Stellungnahme zum Gesetzentwurf zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 2**, S. 22; Kühne/Golla/Schäfer, GSZ 2025, 272 (274); Weizenbaum-Institut, Stellungnahme zur Novellierung des Allgemeinen Sicherheits- und Ordnungsgesetzes Berlin (ASOG Bln), Policy Paper #19, März 2026, S. 23.

Nicht zu erwarten ist, dass statt Echtdaten synthetische Daten genutzt werden. Denn die Erstellung qualitativ hochwertiger synthetischer Daten ist technisch anspruchsvoll und aufwendig,

vgl. Kühne/Golla/Schäfer, GSZ 2025, 272 (274); Kelber/Bortnikov, NJW 2023, 2000 (2002).

Vor diesem Hintergrund hat die Justizministerkonferenz 2025 im Beschluss zur „Ermöglichung der Verwendung von Echtdaten zu Test- und Entwicklungszwecken – Anpassungsbedarf bei den Verfahrensvorschriften“ ausgeführt, dass Test und Training von KI-Systemen mit Echtdaten anstelle von Testdaten vorteilhaft, mitunter sogar zwingend sein kann, um optimale Ergebnisse zu erzielen und den praktischen Anforderungen der Justiz gerecht zu werden,

vgl. Beschluss JMK zum TOP 1.5 vom 5./6. Juni 2025, <https://www.justiz.nrw/sites/default/files/2025-06/TOP%201.05%20-%20Verwendung%20von%20Echtdaten%20zu%20Test-%20und%20Entwicklungs.pdf>

Die Eingriffsintensität erhöht sich auch dadurch, dass nach § 42d Abs. 3 Satz 1 ASOG Polizei und Feuerwehr personenbezogene Daten an Auftragsverarbeitende weitergeben können, wenn eine Verarbeitung durch sie selbst nicht oder nur mit unverhältnismäßigem Aufwand möglich ist. Nach § 42d Abs. 3 Satz 2 ASOG ist gar eine Weitergabe personenbezogener Daten an sonstige Dritte vorgesehen, wenn eine Verarbeitung der Daten durch die Polizei oder Feuerwehr auch unter Zuhilfenahme von Auftragsverarbeitenden nicht oder nur mit unverhältnismäßigem Aufwand möglich ist,

zur Kritik an diesen Regelungen siehe unten cc).

Eine gesetzliche Definition von Auftragsverarbeitenden und Dritten fehlt im ASOG. Wegen des Zusammenhangs zum Datenschutzrecht dürfte auf die Definitionen aus Art. 4 DSGVO und § 31 BlnDSG zurückgegriffen werden. Nach Art. 4 Nr. 8 DSGVO und § 31 Nr. 8 BlnDSG ist Auftragsverarbeiter eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Nach Art. 4 Nr. 10 DSGVO sind Dritte natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.

Diese gesetzliche Ausgestaltung des § 42 Abs. 3 ASOG dürfte regelmäßig auf eine Weiterverarbeitung durch Auftragsverarbeitende bzw. Dritte hinauslaufen. In der Regel dürfte es an verwaltungsinternen Kompetenzen fehlen, die für die Entwicklung, das Training und die Überwachung von KI-Systemen essenziell wären. Angesichts der Gehälter und Arbeitsbedingungen für Spezialisten in der Privatwirtschaft werden Experten auch nur schwer abgeworben werden können,

vgl. Wischmeyer, in: Ebers/Heinze/Krügel/Steinrötter, Künstliche Intelligenz und Robotik, 2. Aufl. 2026, § 22 Rn. 6.

Durch die Übermittlung – ob an Auftragsverarbeiter oder Dritte – entstehen jedoch erhebliche Risiken für die Datensicherheit,

vgl. Botta, Stellungnahme zum Gesetz zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 3**, S. 7.

Die Einhaltung der gesetzlichen Vorgaben – insbesondere hinsichtlich der Geheimhaltung – lässt sich bei Auftragsverarbeitenden und Dritten schwerer nachvollziehen als bei der Polizei bzw. Feuerwehr selbst. Diese Risiken sind auch vor dem Hintergrund der personenbezogenen Daten, die an Auftragsverarbeitende oder Dritte weitergeben werden können, beachtlich. Insoweit sieht § 42d ASOG keine Einschränkungen vor. Es können auch die besonderen Kategorien personenbezogener Daten im Sinne des § 31 Nr. 14 BlnDSG an Dritte weitergegeben werden.

bb) Unzureichende Voraussetzungen

§ 42d ASOG sieht keine hinreichend gehaltvollen Voraussetzungen für den Einsatz von personenbezogenen Test- und Trainingsdaten für KI-Systeme vor,

vgl. Arzt, in: BeckOK PolR NRW, 35. Ed., PolG NRW § 24b Rn. 13 im Erscheinen.

§ 42d Abs. 1 Satz 1 ASOG beschränkt sich auf die Aussage, dass die Daten weiterverarbeitet werden können, „wenn dies erforderlich ist, um KI-Systeme, die der Erfüllung [der] jeweiligen Aufgaben [der Polizei und der Feuerwehr] dienen, unter Verwendung dieser Daten zu trainieren und zu testen“. Die Ziele des Trainings und die Art der zu entwickelnden

KI-Systeme bzw. der möglichen Einsatzszenarien werden nicht spezifiziert,

Berliner Beauftragte für Datenschutz und Informationsfreiheit,
Stellungnahme zum Gesetzentwurf zur Reform des Berliner Polizei-
und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29
der Verfassung von Berlin, **Anlage 2**, S. 21.

Anders als in § 42c Abs. 1 Satz 1 Nr. 1 lit. b) ASOG ist auch nicht Voraussetzung, dass das Interesse an Training und Testung des KI-Systems dem Interesse am Schutz der personenbezogenen Daten überwiegt.

Die Norm ermöglicht somit eine riskante Einspeisung hochsensibler Daten zum Training und zur Testung von KI-Systemen, deren Verwendung gesetzlich nicht explizit vorgesehen ist und die für die polizeilichen Arbeit gegebenenfalls nur einen geringen Vorteil bieten.

Selbst wenn die Anforderungen an den Anlass vor dem Hintergrund des vorbereitenden Charakters des § 42d ASOG geringer sind als bei der anschließenden Maßnahme, die auf dem Einsatz des KI-Systems basiert, entbindet das den Gesetzgeber nicht davon, einen spezifischen Anlass für das Training und den Test von KI-Systemen vorzusehen. Hierzu gehört die zumindest abstrakte Bezeichnung der KI-Systeme, die trainiert oder getestet werden sollen. Der Verweis auf die Aufgabenerfüllung von Polizei und Feuerwehr ist nicht ausreichend. Eine solche generalklauselartige Ermächtigung ist allenfalls bei der Weiterverarbeitung von weniger sensiblen Daten eine taugliche Rechtsgrundlage. Jedenfalls bei der zweckändernden Weiterverarbeitung von sensiblen Daten folgt aus der Wesentlichkeitslehre, dass der parlamentarische Gesetzgeber spezifizieren muss, welche KI-Systeme wie trainiert werden sollen. Das ist vorliegend nicht geschehen.

cc) Unzureichende Schutzvorkehrungen

§ 42d ASOG sieht auch keine hinreichenden Vorkehrungen zum Schutz personenbezogener Daten vor.

§ 42d ASOG sieht insbesondere keine Instrumente vor, um die ohnehin schon unzureichenden Schutzstandards des § 42d ASOG effektiv zu

kontrollieren. Die Norm enthält bereits keine Regelung, nach der dokumentiert werden soll, warum bestimmte Daten für das Training und den Test von KI-Systemen verwendet werden sollen. Die besonderen Protokollierungspflichten des § 27c ASOG beziehen sich nicht auf § 42d ASOG. Ohne eine solche Anforderung kann aber weder eine Behörde noch ein Gericht im Nachhinein effektiv kontrollieren, ob die Anforderungen des § 42d ASOG eingehalten worden sind. Eine solche Dokumentation wäre jedoch umso mehr erforderlich, da die betroffenen Personen über die Verwendung ihrer personenbezogenen Daten für das Training und den Test von KI-Systemen regelmäßig keine Kenntnis haben und daher auf die behördliche und gerichtliche Kontrolle angewiesen sind,

vgl. zu Dokumentationspflichten oben I. 4. b) dd).

§ 42d ASOG sieht im Gesetz selbst auch keine hinreichenden Vorkehrungen hinsichtlich der Art und des Umfangs der zu verarbeitenden Daten, zum technischen Verfahren bzw. zu Sicherungsmaßnahmen vor. Hierbei handelt es sich um grundrechtswesentliche Entscheidungen, die der parlamentarische Gesetzgeber selbst zu treffen hat,

Berliner Beauftragte für Datenschutz und Informationsfreiheit, Stellungnahme zum Gesetzentwurf zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 2**, S. 23.

§ 42d Abs. 4 ASOG überlässt die Festlegung der Anforderung insbesondere zum technischen Verfahren, zu Art und Umfang der zu verarbeitenden Daten und zu Sicherungsmaßnahmen hingegen der Bestimmung durch Verwaltungsvorschriften. Dieser Regelungstechnik ist aber vor dem Hintergrund des potenziell hohen Eingriffsgewichts (siehe oben) nicht ausreichend. § 42d Abs. 4 ASOG kann insbesondere nicht entnommen werden, welches Verfahren zur Verarbeitung von personenbezogenen Daten beim Testen und Trainieren tatsächlich durch die Polizei und die Feuerwehr eingesetzt wird. Die gesetzliche Grundlage beschreibt nicht, welche Prozesse die zunächst von der Polizei erhobenen personenbezogenen Daten beim Auftragsdatenverarbeiter durchlaufen und in welcher Form die so generierten personenbezogenen Daten weiterverarbeitet werden,

vgl. Berliner Beauftragte für Datenschutz und Informationsfreiheit, Stellungnahme zum Gesetzentwurf zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 2**, S. 23.

Unzureichend sind auch die Vorschriften zur Anonymisierung und Pseudonymisierung. Das Stufensystem nach § 42d Abs. 2 ASOG ist zwar im Ansatz tragfähig. Unzureichend ist es jedoch, dass auf eine Anonymisierung bzw. Pseudonymisierung verzichtet werden kann, wenn dies nur mit unverhältnismäßigem Aufwand möglich ist. Laut der Gesetzesbegründung ist der Aufwand der Anonymisierung oder Pseudonymisierung unverhältnismäßig, wenn der Zeit- und Kostenaufwand für die Anonymisierung oder Pseudonymisierung außer Verhältnis steht zu der Zeit- und Kostenersparnis, die durch eine spätere Nutzung des KI-Systems herbeigeführt werden kann,

Abgh-Drs. 19/2553, S. 289.

Der Aufwand soll demnach nicht ins Verhältnis gesetzt werden zu dem Schutz personenbezogener Daten, der durch die Anonymisierung bzw. Pseudonymisierung erreicht werden kann. Die Regelung ermöglicht daher eine rein wirtschaftliche Abwägung und läuft auf eine systematische Verwendung von Klardaten hinaus,

vgl. Berliner Beauftragte für Datenschutz und Informationsfreiheit, Stellungnahme zum Gesetzentwurf zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 2**, S. 22, teilweise zum vergleichbaren § 42d Abs. 3 ASOG; kritisch auch Botta, Stellungnahme zum Gesetz zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 3**, S. 7.

dd) Befugnis zu Weitergabe

§ 42d Abs. 3 ASOG enthält zudem eine zu weitgehende Befugnis zur Weitergabe der Daten an Auftragsverarbeitende und Dritte, ohne ausreichenden Vorkehrungen zu treffen, die gegen den Missbrauch von personenbezogenen Daten schützen.

Das Kriterium, ob eine Verarbeitung durch die Polizei oder Feuerwehr selbst bzw. auch unter Zuhilfenahme Auftragsverarbeitender nur mit unverhältnismäßigem Aufwand möglich ist, ist auch hier zu unbestimmt.

Es grenzt die Übermittlungsbefugnisse nicht ausreichend ein, da es eine rein wirtschaftliche Abwägung ermöglicht,

Berliner Beauftragte für Datenschutz und Informationsfreiheit, Stellungnahme zum Gesetzentwurf zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 2**, S. 22 f; kritisch auch Kipker, BT-Ausschussdrucksache 20(4)493 J, S. 19; Schindler, BT-Ausschussdrucksache 20(4)493 K, S. 21.

Sowohl bei § 42d Abs. 3 Satz 1 als auch Satz 2 ASOG ist das Kriterium jeweils selbstreferentiell. Der Maßstab für die Ermächtigung zur Weitergabe liegt also in den Notwendigkeiten der KI-Verarbeitung und nicht etwa in den Grundrechten der Personen, deren Daten verarbeitet werden.

Jedenfalls die Weitergabe sensibler Daten im Sinne von § 31 Nr. 14 BlnDSG muss ausgeschlossen werden,

vgl. Botta, Stellungnahme zum Gesetz zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 3**, S. 7 f.

Auch der Verweis in § 42d Abs. 3 Satz 4 ASOG auf § 42c Abs. 3, 4 und 5 Satz 1 ASOG stellt keine hinreichende verfahrensrechtliche Absicherung dar. § 42c Abs. 3 ASOG bestimmt, dass personenbezogene Daten nur an Amtsträgerinnen und Amtsträger, für den öffentlichen Dienst besonders Verpflichtete oder an Personen übermittelt werden dürfen, die zur Geheimhaltung verpflichtet worden sind. Wenn die Auftragsverarbeitenden oder Dritten aber einmal über die personenbezogenen Daten verfügen, ist es für die Behörde äußerst schwierig, überhaupt festzustellen, ob die Geheimhaltungspflicht eingehalten wird, geschweige denn Geheimhaltungspflichtverletzungen zu sanktionieren.

Der Verweis in § 42d Abs. 3 Satz 4 ASOG auf § 42c Abs. 4 ASOG bedeutet, dass eine Zweckbindung gilt. Da die Zweckbestimmung „Training und Testung von KI-Systemen“ allerdings denkbar weit ist, führt das zu keiner nennenswerten Begrenzung der Datenverarbeitungsmöglichkeiten.

Durch den Verweis in § 42d Abs. 3 Satz 4 ASOG auf § 42c Abs. 5 Satz 1 Nr. 1 ASOG soll sichergestellt werden, dass die empfangende Stelle organisatorische und technische Maßnahmen gegen unbefugte Kenntnisnahme und zur Einhaltung der Vorgaben des § 51a Abs. 2 ASOG trifft. Auch hier wird es in der Praxis schwierig sein, festzustellen, ob ein Auftragsverarbeitender oder Dritter diesen Anforderungen genügt.

§ 42d Abs. 3 Satz 6 ASOG enthält keine über § 42d Abs. 1 Satz 4 ASOG hinausgehende Aussage. Bereits nach § 42d Abs. 1 Satz 4 ASOG ist eine Weiterverarbeitung personenbezogener Daten, die aus besonders eingriffsintensiven Maßnahmen nach § 42c Abs. 2 ASOG erlangt wurden, ausgeschlossen. Der Ausschluss einer Weiterverarbeitung schließt insbesondere auch eine Weitergabe an Auftragsverarbeitende und Dritte aus.

Schließlich ist es unverhältnismäßig, dass Auftragsverarbeitende und zur Verarbeitung eingesetzte Dritte die trainierten Modelle gemäß § 42d Abs. 3 Satz 8 ASOG für eigene Zwecke weaternutzen dürfen. Damit gehen erhebliche Risiken für die personenbezogenen Daten einher. Wie oben dargelegt, besteht stets das Risiko, dass personenbezogene Daten aus einem KI-Modell abgeleitet werden,

siehe oben aa) und EDSA, Stellungnahme 28/2024 zu gewissen Datenschutzaspekten der Verarbeitung personenbezogener Daten im Zusammenhang mit KI-Modellen, 2024, S. 15 f., Rn. 31 ff.

Können Dritte die Modelle zu beliebigen Zwecken weaternutzen, steigt das Risiko exponentiell. Im Ergebnis besteht die Gefahr, dass sehr sensible Daten, die mit eingriffsintensiven polizeilichen Methoden erhoben wurden, in die falschen Hände geraten.

Dieses Risiko wird durch die Einschränkungen in § 42d Abs. 3 Satz 8 ASOG nicht ausgeschlossen. Danach dürfen die Modelle nur weitergenutzt werden, wenn Polizei oder Feuerwehr dem zugestimmt haben und sichergestellt werden kann, dass aus den trainierten Modellen keine Trainingsdaten abgeleitet werden können. Das ist in dreifacher Hinsicht unzureichend.

Erstens genügt nach dem Wortlaut, dass sichergestellt werden *kann*, dass aus den trainierten Modellen keine Trainingsdaten abgeleitet werden können. Keine Voraussetzung ist, dass dies sichergestellt *ist*. Laut der Gesetzesbegründung muss zwar sichergestellt sein, dass die Ausgangsdaten, die dem Training dienten, nicht wiederhergestellt werden können,

Abgh-Drs. 19/2553, S. 290.

Im Gesetzestext kommt das aber nicht zum Ausdruck.

Zweitens bezieht sich die „Sicherstellung“ nur auf die Ableitung von Trainingsdaten. KI-Modelle enthalten in der Regel jedoch keine Aufzeichnungen, sondern „Parameter, die probabilistische Beziehungen zwischen den im Modell enthaltenen Daten darstellen“. Auch in diesen Fällen ist es möglich, Daten aus dem Modell abzuleiten, die zwar ungenau sein mögen, aber dennoch einen Personenbezug aufweisen,

EDSA, Stellungnahme 28/2024 zu gewissen Datenschutzaspekten der Verarbeitung personenbezogener Daten im Zusammenhang mit KI-Modellen, 2024, S. 15 f., Rn. 37 ff.

Drittens ist die Beurteilung der Anonymisierung bei KI-Modellen komplex und erfordert eine gründliche Prüfung,

EDSA, Stellungnahme 28/2024 zu gewissen Datenschutzaspekten der Verarbeitung personenbezogener Daten im Zusammenhang mit KI-Modellen, 2024, S. 15 f., Rn. 40.

Eine solche Prüfung kann nur mit technischem Sachverstand durchgeführt werden. Wegen des hohen Risikos muss die Prüfung zudem einer unabhängigen Stelle vorbehalten sein. Erforderlich wäre daher ein Zustimmungsvorbehalt oder zumindest eine Beteiligungsgebot zugunsten der Landesbeauftragten für den Datenschutz. § 42d Abs. 3 Satz 8 ASOG macht die Weiternutzung durch Dritte hingegen nur von einer Zustimmung der Polizei oder Feuerwehr abhängig.

VI. § 47a ASOG (automatisierte Datenanalyse)

§ 47a ASOG verstößt gegen das IT-Grundrecht aus Art. 7 VvB i.V.m. Art. 6 Satz 1 VvB, das Fernmeldegeheimnis aus Art. 16 VvB, die Unverletzlichkeit der Wohnung aus Art. 28 Abs. 2 VvB sowie gegen das Recht auf informationelle Selbstbestimmung aus Art. 33 VvB.

Die Norm schafft eine Rechtsgrundlage für die automatisierte Datenanalyse durch die Berliner Polizei. Hierfür werden zunächst rechtmäßig gespeicherte personenbezogene Daten auf einer Analyseplattform zusammengeführt, verknüpft und aufbereitet. Auf dieser Grundlage erfolgt sodann die automatisierte Datenanalyse; unter bestimmten Voraussetzungen dürfen hierfür auch selbstlernende KI-Systeme eingesetzt werden (1.). Die Befugnis ist anbieteroffen, sodass auch die Nutzung der Software Gotham des US-Unternehmens Palantir ermöglicht wird (2.).

Sowohl die Zusammenführung personenbezogener Daten auf der Analyseplattform als auch die anschließende automatisierte Datenanalyse stellen eigenständige Eingriffe in diejenigen Grundrechte dar, in die bereits durch die ursprüngliche Datenerhebung eingegriffen wurde (3.). Diese Eingriffe sind nicht gerechtfertigt (4.). Bereits die Erstellung der Analyseplattform ist unverhältnismäßig, weil sie ohne Eingriffsvoraussetzungen die weitreichende Zusammenführung personenbezogener Daten ermöglicht und keine ausreichenden Vorgaben zur Zweckbindung und Kennzeichnung enthält (4. a)). Auch die automatisierte Datenanalyse genügt den verfassungsrechtlichen Anforderungen nicht. Angesichts ihres hohen Eingriffsgewichts (4. b) aa)) fehlen hinreichend bestimmte Eingriffsvoraussetzungen (4. b) bb)), Kennzeichnungspflichten (4. b) cc)), ausreichende Vorkehrungen gegen Fehler, Diskriminierung und Datenmissbrauch (4. b) dd)) sowie wirksame datenschutzrechtliche Kontrollmechanismen (4. b) ee)).

1. Gesetz und Gesetzesbegründung

Der neu eingeführte § 47a ASOG schafft erstmals eine Rechtsgrundlage für die automatisierte Datenanalyse durch die Berliner Polizei.

Vorgesehen ist ein zweistufiges Verfahren. Zunächst werden personenbezogene Daten zur Vorbereitung der automatisierten Datenanalyse zusammengeführt (§ 47a Abs. 1 Satz 1 ASOG). Hierdurch wird eine Analyseplattform generiert. Mithilfe dieser Datenbank erfolgt sodann im zweiten Schritt die automatisierte Datenanalyse (§ 47a Abs. 1 Satz 2 ASOG). Dabei ist auch der Einsatz selbstlernender KI-Systeme zulässig (§ 47a Abs. 1 Satz 5 ASOG). § 47a Abs. 4 ASOG begründet eine gegenüber § 42d ASOG speziellere Rechtsgrundlage für das Testen der automatisierten Datenanalyse mit personenbezogenen Daten.

Die Norm hat folgenden Wortlaut:

§ 47a

Automatisierte Anwendung zur Analyse vorhandener Daten

(1) Die Polizei kann rechtmäßig gespeicherte personenbezogene Daten ausschließlich zur Vorbereitung der automatisierten Datenanalyse nach Absatz 2 Satz 1 auf einer Analyseplattform automatisiert zusammenführen, verknüpfen und aufbereiten. Diese zusammengeführten Daten kann die Polizei, auch gemeinsam mit weiteren rechtmäßig erhobenen personenbezogenen Daten, nach Absatz 2 Satz 2 verknüpfen, aufbereiten und auswerten sowie für statistische Zwecke anwenden (automatisierte Datenanalyse),

1. wenn die Maßnahme zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes, für Leib, Leben, Freiheit oder sexuelle Selbstbestimmung einer Person oder für Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, erforderlich ist,

2. wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass innerhalb eines übersehbaren Zeitraumes auf eine zumindest ihrer Art nach konkretisierte Weise

a) eine terroristische Straftat oder

b) eine in § 100a Absatz 2 der Strafprozessordnung genannte und voraussichtlich auch im Einzelfall schwerwiegende Straftat

begangen werden soll und die Maßnahme zur Verhütung dieser Straftat erforderlich ist, oder

3. wenn das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums eine terroristische Straftat begehen oder an ihr teilnehmen wird, und die Maßnahme zur Verhütung dieser Straftat erforderlich ist.

In den Fällen des Satzes 2 ist die Maßnahme nur zulässig, wenn sie nicht außer Verhältnis zur Bedeutung des aufzuklärenden Sachverhalts steht. Die automatisierte Anwendung zur Auswertung vorhandener Daten erfolgt anhand von Suchbegriffen, die sich aus einem konkreten Sachverhalt, bezogen auf einen Anlass im Sinne des Satzes 2 ergeben. Unter den Voraussetzungen von Satz 2 Nummer 1 und 3 ist auch die Nutzung selbstlernender Systeme zulässig, im

Übrigen jedoch nur, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass innerhalb eines übersehbaren Zeitraumes auf eine zumindest ihrer Art nach konkretisierte Weise

1. eine terroristische Straftat oder

2. eine in § 100b Absatz 2 der Strafprozessordnung genannte und voraussichtlich auch im Einzelfall besonders schwerwiegende Straftat

begangen werden soll und die Maßnahme zur Verhütung dieser Straftat erforderlich ist. Es ist durch geeignete Maßnahmen sicherzustellen, dass bei der automatisierten Datenanalyse diskriminierende Algorithmen weder herausgebildet noch verwendet werden. Es werden nur mit den Suchparametern übereinstimmende Daten angezeigt. Automatisierte Entscheidungsfindungen und Sachverhaltsbewertungen sind unzulässig. Alle Ergebnisse der automatisierten Datenanalyse müssen aus den in Absatz 2 Satz 1 bis 4 genannten Daten durch menschliche Gedankengänge nachvollziehbar sein. Sollen in der Folge der automatisierten Datenanalyse Maßnahmen gegen Personen getroffen werden, dürfen diesen Maßnahmen allein Daten in einer nicht nach dem hiesigen Absatz verarbeiteten Fassung zugrunde gelegt werden.

(2) Bei der automatisierten Datenanalyse können auf der Analyseplattform rechtmäßig gespeicherte Vorgangsdaten, Falldaten, Daten aus den polizeilichen Auskunftssystemen, Telekommunikationsdaten, Daten aus Asservaten, Daten aus dem polizeilichen Informationsaustausch, soweit sie der polizeilichen Aufgabenerfüllung dienen, und in den Fällen des Absatzes 1 Satz 2 Nummer 1 auch Nutzungs- und Verkehrsdaten weiterverarbeitet werden. Datensätze aus gezielten Abfragen in Datenverbünden der Polizei und gesondert geführten staatlichen Registern können, auch automatisiert, erhoben und in die Weiterverarbeitung einbezogen werden. Eine direkte Anbindung an Internetdienste mit Ausnahme geschlossener behördlicher Datennetze ist ausgeschlossen. Einzelne gesondert gespeicherte Datensätze aus Internetquellen können in die Weiterverarbeitung einbezogen werden. Nicht in die Datenanalyse einbezogen werden Vorgangsdaten von Unbeteiligten. § 42a Absatz 1 bis 4, § 42b und § 42c Absatz 1 gelten entsprechend; § 48 bleibt unberührt. In einem Konzept der Kategorisierung und Kennzeichnung personenbezogener Daten ist anhand der Maßstäbe des Veranlassungszusammenhangs und der Grundrechtsrelevanz vorzusehen, welche personenbezogenen Daten in welcher Weise in eine automatisierte Anwendung zur Datenanalyse einbezogen werden dürfen. Die Höchstspeicherdauer richtet sich nach den Speicherfristen der Ursprungsdaten. Für Verkehrsdaten in der Analyseplattform beträgt sie höchstens zwei Jahre, sofern die Daten nicht für die Fallbearbeitung weiter benötigt werden.

(3) Zugriff auf die automatisierte Datenanalyse dürfen nur ausgewählte und geschulte Polizeidienstkräfte haben. Werden selbstlernende Systeme eingesetzt, so darf die automatisierte Datenanalyse nur durch die Leitung des Landeskriminalamtes, deren Vertretung im Amt oder durch von dieser besonders beauftragte Beamtinnen oder Beamte des höheren Dienstes angeordnet werden. Durch organisatorische und technische Maßnahmen sind die Zugriffsmöglichkeiten der eingesetzten Polizeidienstkräfte auf das erforderliche Maß zu beschränken. In einem Rollen- und Rechtekonzept ist die zweckabhängige Verteilung der Zugriffsrechte zu bestimmen; diese müssen sachlich auf das erforderliche Maß eingeschränkt werden. Die Zugriffe sind zu begründen und zu protokollieren; dabei ist auch das Vorliegen der Voraussetzungen nach den Absätzen 1 und 2 zu dokumentieren. Personen, deren personenbezogene Daten nach Absatz 1 weiterverarbeitet wurden und gegen die anschließend weitere Maßnahmen nach diesem Gesetz getroffen wurden, sind nach Abschluss der Folgemaßnahmen gemäß § 42 des Berliner Datenschutzgesetzes über die

Datenverarbeitung nach Absatz 1 zu benachrichtigen; § 27d Absatz 2, 3 und 5 gilt entsprechend. Die oder der behördliche Datenschutzbeauftragte führt spätestens alle zwei Jahre stichprobenartige Kontrollen durch.

(4) Die Polizei kann von ihr rechtmäßig gespeicherte personenbezogene Daten nach Absatz 2 Satz 1 und 2 weiterverarbeiten, wenn dies erforderlich ist, um die automatisierte Datenanalyse zu testen. Personenbezogene Daten sind für die Verwendung zu Testzwecken zu anonymisieren. Kann der Zweck des Tests mit anonymisierten Daten nicht erreicht werden oder ist die Anonymisierung nur mit unverhältnismäßigem Aufwand möglich, sind die Daten zu pseudonymisieren. Kann der Zweck des Tests auch mit pseudonymisierten Daten nicht erreicht werden oder ist auch die Pseudonymisierung nur mit unverhältnismäßigem Aufwand möglich, dürfen personenbezogene Daten verwendet werden. Besondere Kategorien personenbezogener Daten dürfen nur unter Beachtung des § 51a Absatz 2 verwendet werden. Die Weiterverarbeitung von personenbezogenen Daten, die durch einen verdeckten Einsatz technischer Mittel in oder aus Wohnungen oder durch einen verdeckten Eingriff in informationstechnische Systeme erlangt wurden, ist unzulässig.

(5) Die Einrichtung und jede wesentliche Änderung der automatisierten Datenanalyse erfolgen durch Anordnung der Polizeipräsidentin oder des Polizeipräsidenten oder der Vertretung im Amt; diese Befugnis kann auf die Leitung des Landeskriminalamtes oder ihre Vertretung im Amt übertragen werden. Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit ist vor der Einrichtung oder wesentlichen Änderungen nach Satz 1 anzuhören; bei Gefahr im Verzug ist die Anhörung unverzüglich nachzuholen. Im Übrigen bleiben die Aufgaben und Befugnisse der oder des Berliner Beauftragten für Datenschutz und Informationsfreiheit unberührt.

(6) Das Nähere zu den Absätzen 2 bis 4 bestimmen zu veröffentlichende Verwaltungsvorschriften. Die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit ist vor dem Erlass oder einer Änderung der Verwaltungsvorschriften anzuhören.

(7) Der Senat unterrichtet das Abgeordnetenhaus jährlich über die nach Absatz 1 getroffenen Maßnahmen. In dem Bericht ist insbesondere darzustellen, in welchem Umfang von den Maßnahmen aus Anlass welcher Gefahrenlagen Gebrauch gemacht wurde. Die parlamentarische Kontrolle auf der Grundlage dieses Berichts wird von einem Kontrollgremium ausgeübt. Die Vorschriften des Fünften Abschnitts des Verfassungsschutzgesetzes Berlin gelten entsprechend.

Nach der Gesetzesbegründung schafft der neue § 47a ASOG eine Rechtsgrundlage dafür, bisher unverbundene, automatisierte Dateien und Datenquellen in Analyseplattformen zusammenzuführen und die vorhandenen Datenbestände durch Suchfunktionen systematisch zu erschließen. Das sei erforderlich, weil sich auch in der Polizei Berlin die IT-Struktur mit verschiedenen Datensammlungen in teilweise verschiedenen Dateiformaten organisch entwickelt habe. Als Folge davon setze eine übergreifende Auswertung zunächst eine zeit- und ressourcenaufwendige Abfrage in den jeweiligen Datensystemen sowie ein anschließendes Zusammenführen der Daten voraus,

Abgh-Drs. 19/2553, S. 329.

Die Gesetzesbegründung nimmt Bezug auf die Entscheidung des Bundesverfassungsgerichts vom 16. Februar 2023 zur automatisierten Datenanalyse zum hessischen und hamburgischen Polizeirecht. Der Entwurf orientiere sich an § 25a HSOG und § 49 PolDVG Hamburg in der Fassung, wie sie im Anschluss an das Urteil des Bundesverfassungsgerichts überarbeitet wurde,

Abgh-Drs. 19/2553, S. 329.

Bei der Wahl des Anbieters für die automatisierte Datenanalyse seien die Grundsätze der digitalen Souveränität zu beachten und jegliche Abhängigkeiten oder Einflussnahmen zu vermeiden, insbesondere von Unternehmen, Einrichtungen oder sonstigen Stellen, die ihren Sitz nicht innerhalb der Europäischen Union oder einem Schengen-assoziierten Staat haben,

Abgh-Drs. 19/2553, S. 329 f.

2. Funktionsweise und Anwendungsszenarien

Eine Regelung darüber, welcher Anbieter das System zur automatisierten Datenanalyse bereitstellen soll, sieht § 47a ASOG nicht vor. Die Norm ist anbieteroffen.

Mehrere Bundesländer nutzen bereits die Software Gotham des US-Unternehmens Palantir als sogenannte „Verfahrensübergreifenden Recherche- und Analyseplattform“ („VeRA“). Die Software steht in der Kritik, da sie die Vernetzung großer, bislang getrennt gespeicherter Datenbestände in besonderem Maße erleichtert und dadurch die Erstellung umfassender Personen- und Beziehungsprofile ermöglicht. Zudem werden eine Abhängigkeit staatlicher Stellen von einem privaten US-amerikanischen Anbieter (Vendor Lock-in), Defizite bei Transparenz und demokratischer Kontrolle sowie Fragen der digitalen Souveränität angeführt.

Im Rahmen der parlamentarischen Debatte im Abgeordnetenhaus wurde zwar darauf verwiesen, dass zur automatisierten Datenanalyse auf einen Anbieter wie Palantir nicht zurückgegriffen werden soll,

vgl. Abgh, Plenarprotokoll 19/69, S. 13.

Nach dem Gesetz ist dies jedoch nicht ausgeschlossen.

3. Eingriffe in den Schutzbereich

§ 47a Abs. 1 ASOG begründet zwei separate Eingriffe in das IT-Grundrecht aus Art. 7 VvB i.V.m. Art. 6 Satz 1 VvB, das Fernmeldegeheimnis aus Art. 16 VvB, die Unverletzlichkeit der Wohnung nach Art. 28 Abs. 2 VvB und das Recht auf informationelle Selbstbestimmung aus Art. 33 VvB.

Zum einen stellt bereits das Zusammenführen, Verknüpfen und Aufbereiten von personenbezogenen Daten auf der Analyseplattform nach § 47a Abs. 1 Satz 1 ASOG einen Eingriff dar,

vgl. Bäuerle, in: BeckOK Polizei- und Ordnungsrecht Hessen, 38. Edition, Stand 1.4.2026, § 25a Rn. 100; Berliner Beauftragte für Datenschutz und Informationsfreiheit, Stellungnahme zum Gesetzentwurf zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 2**, S. 25; Berliner Beauftragte für Datenschutz und Informationsfreiheit, Stellungnahme zum Änderungsantrag der Fraktion der CDU und der Fraktion der SPD zur Drucksache 19/2553: Gesetz zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 7**, S. 3; Botta, Stellungnahme zum Gesetz zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 3**, S. 14.

Die Zusammenführung erfolgt gezielt und allein zum Zwecke der weiteren Verarbeitung,

Arzt, in: BeckOK PolR NRW, 34. Ed. 15.4.2026, PolG NRW § 23 Rn. 56 mit Verwies auf BVerfGE 150, 244 <266 Rn. 43>; vgl. zur Grundrechtsrelevanz der Trennung bzw. Zusammenführung von Daten: BVerfGE 115, 320 <342 f. Rn. 72>; 156, 11 <39 f. Rn. 73>; EuGH, Urt. v. 30.04.2024, C-470/21, La Quadrature du Net u. a. gegen Premier Ministre, Ministre de la Culture, ECLI:EU:C:2024:370, Rn. 84.

Zum anderen begründet die nachgelagerte automatisierte Datenanalyse nach § 47a Abs. 2 Satz 2 ASOG einen eigenständigen Eingriff.

§ 47a Abs. 1 Satz 1 und Satz 2 ASOG erlauben die zweckändernde Weiterverarbeitung von bereits erhobenen personenbezogenen Daten, da die Erhebungsbefugnisse keine derartigen Zwecke kennen. Sie greifen in die Grundrechte ein, in die durch die ursprüngliche Datenerhebung eingegriffen wurde,

siehe dazu oben IV. 3.

Die Daten für die Erstellung der Analyseplattform und die automatisierte Datenanalyse können durch verschiedene polizeiliche Maßnahmen erhoben worden sein. Über die Herkunft der Daten trifft § 47a Abs. 2 Satz 1 ASOG keine Aussage. Die Norm regelt allein die Art der Daten, die bei der automatisierten Datenanalyse verwendet werden können. Die Ausnahme nach § 47a Abs. 4 Satz 6 ASOG bezieht sich ausweislich der systematischen Stellung allein auf die Testung der automatisierten Datenanalyse nach § 47a Abs. 4 ASOG. Der Verweis in § 47a Abs. 2 Satz 6 ASOG auf § 42a Abs. 3 ASOG verdeutlicht, dass selbst Daten, die mit den dort genannten schwerwiegenden Grundrechtseingriffen erlangt wurden, grundsätzlich für die automatisierte Datenanalyse verwendet werden können,

vgl. Abgh-Drs. 19/2553 S. 334 f.

Für die Maßnahmen nach § 47a ASOG können daher unten anderem Daten verwendet werden, die durch Telekommunikationsüberwachung (§ 26 ASOG, Eingriff in Art. 16 VvB), eine Quellen-Telekommunikationsüberwachung oder Online-Durchsuchung (§§ 26a, 26b ASOG, Eingriff in das IT-Grundrecht aus Art. 7 VvB i.V.m. Art. 6 Satz 1 VvB und Art. 16 VvB) oder durch eine Wohnraumüberwachung oder Wohnungsdurchsuchung (§§ 25b, 36 ASOG, Eingriff in Art. 28 Abs. 2 Satz 1 VvB) erhoben worden sind. Im Übrigen handelt es sich jedenfalls um Daten, die unter Eingriff in das Recht aus Art. 33 VvB erhoben worden sind.

4. Keine Rechtfertigung

Die Eingriffe sind nicht gerechtfertigt. Das gilt sowohl für die Erstellung der Analyseplattform (a)) als auch für die automatisierte Datenanalyse (b)).

a) Analyseplattform

Die Erstellung der Analyseplattform dient zwar einem legitimen Zweck und ist auch geeignet, indem sie die automatisierte Analyse vorbereitet. Zweifelhaft ist jedoch die Erforderlichkeit, da ein milderer Mittel die ad-hoc-Zusammenführung der für den jeweiligen Sachverhalt relevanten Datenbestände für die Durchführung der automatisierten Datenanalyse ist.

Jedenfalls ist die Erstellung der Analyseplattform unverhältnismäßig im engeren Sinne. Der Eingriff ist jedenfalls von erheblicher Intensität (aa)). § 47a Abs. 1 Satz 1 ASOG sieht keine korrespondierenden Eingriffsvoraussetzungen vor (bb)). Außerdem ist keine Kennzeichnung der Daten vorgesehen (cc)).

aa) Eingriffsintensität

Der mit § 47a Abs. 1 Satz 1 ASOG verbundene Eingriff durch die Erstellung einer Analyseplattform wiegt schwer,

siehe im Ergebnis Botta, Stellungnahme zum Gesetz zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 3**, S. 14; Weizenbaum-Institut, Stellungnahme zur Novellierung des Allgemeinen Sicherheits- und Ordnungsgesetzes Berlin (ASOG Bln), Policy Paper #19, März 2026, S. 26.

Dies folgt insbesondere daraus, dass Art und Umfang der Daten, die für die Erstellung der Analyseplattform verwendet werden können, kaum Begrenzungen erfahren haben.

Die Analyseplattform kann mit nahezu allen polizeilichen verfügbaren Datenbeständen gespeist werden. Voraussetzung ist lediglich, dass sie rechtmäßig gespeichert sind.

§ 47a Abs. 1 Satz 1 ASOG enthält – im Unterschied zur anschließenden Datenanalyse nach § 47a Abs. 1 Satz 2 ASOG – keine Bestimmung dazu, welche Datenarten in welchem Umfang zur Erstellung der Analyseplattform genutzt werden dürfen,

vgl. Bäuerle, in: BeckOK Polizei- und Ordnungsrecht Hessen, 38. Edition, Stand 1.4.2026, § 25a Rn. 51.

§ 47a Abs. 2 Satz 1 ASOG bezieht sich nach dessen eindeutigem Wortlaut („Bei der automatisierten Datenanalyse“) allein auf den Eingriff nach § 47a Abs. 1 Satz 2 ASOG. Als automatisierte Datenanalyse bezeichnet der Gesetzgeber ausweislich der Legaldefinition in § 47a Abs. 1 Satz 2 ASOG nur die auf der Analyseplattform aufbauende Analyse. Diese Unterscheidung wird auch dadurch deutlich, dass der Gesetzgeber sich in anderen Bestimmungen, wie z.B. § 47a Abs. 2 Satz 9 ASOG, ausdrücklich auf die Analyseplattform an sich bezieht.

Vor diesem Hintergrund können auch Vorgangsdaten von Unbeteiligten unbegrenzt für die Erstellung der Analyseplattform genutzt werden. Die Einschränkung des § 47a Abs. 2 Satz 5 ASOG gilt ausdrücklich nur für die „Datenanalyse“.

Eine Eingrenzung der einbeziehbaren Daten folgt auch nicht – jedenfalls nicht mit hinreichender Bestimmtheit – daraus, dass § 47a Abs. 1 Satz 1 ASOG auf § 47a Abs. 2 Satz 1 ASOG verweist. Denn dieser Verweis bezieht sich nicht auf die einbeziehbaren Daten, sondern auf den Zweck der Zusammenführung („zur Vorbereitung der automatisierten Datenanalyse nach Absatz 2 Satz 1“).

Die Gesetzesbegründung geht zwar davon aus, dass nur Daten nach § 47a Abs. 2 Satz 1 ASOG dauerhaft auf der Analyseplattform gespeichert werden,

Abgh-Drs. 19/2553, S. 331.

Dem Gesetz lässt sich eine solche Beschränkung jedoch nicht mit hinreichender Bestimmtheit entnehmen,

ebenso Berliner Beauftragte für Datenschutz und Informationsfreiheit, Stellungnahme zum Änderungsantrag der Fraktion der CDU und der Fraktion der SPD zur Drucksache 19/2553: Gesetz zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 7**, S. 26: „Unklar bleibt, worunter die Datenerhebungen aus den Eingriffsbefugnissen zu fassen sind.“

Selbst wenn die Norm derart ausgelegt werden sollte, dass sich die Beschränkungen hinsichtlich der Art der Daten auch auf die Erstellung der Analyseplattform beziehen, würde das nicht zu einer merklichen

Minimierung des Eingriffsgewichts führen. Denn auch in diesem Fall könnten sehr viele, teils sehr sensible Daten zusammengeführt, verknüpft und aufbereitet werden,

siehe ausführlich unten b) aa) (i).

Nicht hinreichend bestimmt geregelt ist, ob sich die Einschränkung des § 47a Abs. 2 Satz 3 ASOG auch auf die Erstellung der Analyseplattform bezieht. Danach ist eine direkte Anbindung an Internetdienste mit Ausnahme geschlossener behördlicher Datennetze ausgeschlossen. Dies würde sich zwar eingriffsmildernd auswirken. Der Effekt wird allerdings dadurch relativiert, dass nach § 47a Abs. 2 Satz 4 ASOG gespeicherte Datensätze aus Internetquellen einbezogen werden können. So können händisch – auch in großer Anzahl – Daten aus Internetquellen, wie Social Media, auch für die Erstellung der Analyseplattform genutzt werden,

vgl. Botta, Stellungnahme zum Gesetz zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 3**, S. 13.

Im Ergebnis wird es der Polizei ermöglicht, eine „Super-Datenbank“ zu erstellen,

Botta, Stellungnahme zum Gesetz zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 3**, S. 14.

Diese dürfte im Ergebnis zudem dauerhaft bestehen. Zwar unterliegen die zusammengeführten Daten nach § 47a Abs. 2 Satz 8 und 9 ASOG Löschfristen. Dennoch besteht die Besonderheit gegenüber der vom Bundesverfassungsgericht 2023 entschiedenen Konstellation darin, dass die Analyseplattform an sich verstetigt und nicht ad-hoc erstellt werden soll. Gerade diese Verstetigung wirkt eingriffserhöhend,

vgl. Stellungnahme der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum Entwurf eines Gesetzes zur Verbesserung der Terrorismusbekämpfung, BT-Drs. 20/12806, S. 8.

Die Begrenzungen des § 47a Abs. 3 ASOG beziehen sich schon wegen des Wortlauts nicht auf die Analyseplattform nach § 47a Abs. 1 Satz 1 ASOG. Dasselbe gilt für § 47a Abs. 5 ASOG.

Das Eingriffsgewicht bei der Erstellung der Analyseplattform nach § 47 Abs. 1 Satz 1 ASOG steigt auch dadurch, dass die Betroffenen, deren personenbezogene Daten hierfür genutzt werden, hierüber nicht informiert werden. Die Informationspflicht nach § 47a Abs. 3 Satz 6 ASOG greift nur, wenn gegen die Person anschließend weitere Maßnahmen nach dem ASOG getroffen werden. Das dürfte aber im Rahmen der Erstellung der Analyseplattform die Ausnahme sein. Auch die Benachrichtigungspflicht nach § 27d Abs. 1 ASOG greift nicht. Diese bezieht sich nicht auf § 47a ASOG.

bb) Keine ausreichenden Voraussetzungen

§ 47a Abs. 1 Satz 1 ASOG enthält keine dem Eingriffsgewicht entsprechenden Eingriffsvoraussetzungen.

Grundsätzlich muss bei schwerwiegenden Grundrechtseingriffen mindestens eine konkretisierte Gefahr für besonders gewichtige Rechtsgüter vorliegen,

siehe oben II. 4. b) und BVerfG, Urteil des Ersten Senats vom 16. Februar 2023 – 1 BvR 1547/19 –, Rn. 105 f.

Selbst wenn man bei der Analyseplattform mit Blick auf den vorbereitenden Charakter von einem weniger gewichtigen Eingriff ausgeht, wäre erforderlich, dass die Norm entweder eine konkretisierte Gefahr oder den Schutz besonders gewichtiger Rechtsgüter voraussetzt,

BVerfG, Urteil des Ersten Senats vom 16. Februar 2023 – 1 BvR 1547/19 –, Rn. 107.

Mindestens wären nach den Grundsätzen über die Zweckbindung der Schutz entsprechend gewichtiger Rechtsgüter und ein konkreter Ermittlungsansatz erforderlich,

siehe oben V. 4. a) und BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, Rn. 289.

Diesen Voraussetzungen genügt § 47a Abs. 1 Satz 1 ASOG nicht im Ansatz. Die einzige Eingrenzung in § 47a Abs. 1 Satz 1 ASOG ist, dass die Zusammenführung der gespeicherten Daten „ausschließlich zur Vorbereitung der automatisierten Datenanalyse nach Absatz 2 Satz 1“

erfolgen darf. Diese Eingrenzung des Zwecks der Weiterverarbeitung genügt offensichtlich nicht den Grundsätzen der Zweckbindung und hypothetischen Datenneuerhebung. Die Norm berücksichtigt in keiner Weise den Anlass für die ursprüngliche Datenerhebung. Auch knüpft sie die Erstellung der Analyseplattform nicht an den Schutz gewichtiger Rechtsgüter oder an eine konkretisierte Gefahr.

Die Eingriffsvoraussetzungen nach § 47a Abs. 1 Satz 2 ASOG greifen erst bei der anschließenden automatisierten Datenanalyse,

vgl. Berliner Beauftragte für Datenschutz und Informationsfreiheit, Stellungnahme zum Gesetzentwurf zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 2**, S. 25; Weizenbaum-Institut, Stellungnahme zur Novellierung des Allgemeinen Sicherheits- und Ordnungsgesetzes Berlin (ASOG Bln), Policy Paper #19, März 2026, S. 26; vgl. zu § 25a Abs. 1 Satz 1 HSOG: Bäuerle, in: BeckOK PolR Hessen, 39. Ed. 1.7.2026, HSOG § 25a Rn. 100.

Dies ist eine bewusste Entscheidung des Gesetzgebers und kann auch nicht durch eine verfassungskonforme Auslegung kompensiert werden. Im Gesetzgebungsverfahren hat unter anderem die Berliner Beauftragte für Datenschutz und Informationsfreiheit auf dieses Problem hingewiesen. Ungeachtet dessen hat der Gesetzgeber § 47a ASOG insoweit nicht verändert,

vgl. Berliner Beauftragte für Datenschutz und Informationsfreiheit, Stellungnahme zum Änderungsantrag der Fraktion der CDU und der Fraktion der SPD zur Drucksache 19/2553: Gesetz zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 7**, S. 3.

Vielmehr hat der Gesetzgeber allein aufgenommen, dass die automatisierte Zusammenführung, Verknüpfung und Aufbereitung der Daten „ausschließlich der Vorbereitung der automatisierten Datenanalyse“ dient,

Änderungsantrag der Fraktion der CDU und der Fraktion der SPD zur Drucksache 19/2553, **Anlage 6**, S. 41.

Zwar verweist § 47a Abs. 2 Satz 6 ASOG auf die Regelung über zweckwahrende und zweckändernde Datenverarbeitung, § 42a ASOG. Da § 47a Abs. 2 ASOG sich aber nur auf die automatisierte

Datenanalyse bezieht und nicht auf die Zusammenführung in § 47a Abs. 1 Satz 1 ASOG, gelten die Begrenzungen des § 42a ASOG nicht bereits für die zweckändernde Zusammenführung,

vgl. Berliner Beauftragte für Datenschutz und Informationsfreiheit, Stellungnahme zum Gesetzentwurf zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 2**, S. 25.

cc) Fehlende Kennzeichnung

Es fehlt zudem an einer verpflichtenden Kennzeichnung der in der Analyseplattform zusammengeführten Daten.

§ 47a Abs. 2 Satz 6 ASOG enthält zwar einen Verweis auf die Regelungen über die Zweckbindung und Kennzeichnung nach §§ 42a, 42b ASOG. Dieser Verweis gilt jedoch ebenfalls nur für die automatisierte Datenanalyse nach § 47a Abs. 1 Satz 2 ASOG, nicht für die Erstellung der Analyseplattform,

vgl. Berliner Beauftragte für Datenschutz und Informationsfreiheit, Stellungnahme zum Gesetzentwurf zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 2**, S. 25.

Vor diesem Hintergrund fehlen insbesondere Vorkehrungen zur Kennzeichnung von personenbezogenen Daten, wie sie § 42d ASOG vorsieht. Vielmehr kann nahezu der sämtliche polizeiliche Datenbestand ohne Kennzeichnung zu einer Analyseplattform zusammengeführt werden.

Auch dies ist eine bewusste Entscheidung des Gesetzgebers und kann nicht durch eine verfassungskonforme Auslegung kompensiert werden. Auf diesen Umstand hat im Gesetzgebungsverfahren unter anderem die Berliner Beauftragte für Datenschutz und Informationsfreiheit hingewiesen. Der Gesetzgeber hat § 47a ASOG jedoch insoweit nicht angepasst,

vgl. Berliner Beauftragte für Datenschutz und Informationsfreiheit, Stellungnahme zum Änderungsantrag der Fraktion der CDU und der Fraktion der SPD zur Drucksache 19/2553: Gesetz zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 7**, S. 3.

Selbst wenn sich der Verweis von § 47a Abs. 2 Satz 6 ASOG auf § 42b ASOG auch auf die Erstellung der Analyseplattform beziehen würde, enthält § 42b Abs. 4 ASOG zu weitgehende Ausnahmen von der Kennzeichnungspflicht und dem damit korrespondierenden Verbot der Weiterverarbeitung nicht gekennzeichnete Daten,

siehe oben IV.

b) Datenanalyse

Auch der Eingriff durch die automatisierte Datenanalyse nach § 47a Abs. 1 Satz 2 ASOG ist nicht gerechtfertigt. Der Eingriff wiegt schwer (aa)). Es fehlt an hinreichend gehaltvollen Voraussetzungen (bb)), einer ausreichenden Kennzeichnungspflicht für die verwendeten Daten (cc)), Vorkehrungen gegen Fehler, Diskriminierung und Datenmissbrauch (dd)) und ausreichenden datenschutzrechtlichen Kontrollen (ee)).

aa) Eingriffsintensität

Der mit der automatisierten Datenanalyse verbundene Eingriff nach § 47a Abs. 1 Satz 2 ASOG wiegt schwer. Art und Umfang der Daten, die für die automatisierte Datenanalyse nach § 47a Abs. 1 Satz 2 ASOG verwendet werden können, sind kaum begrenzt ((i)). Auch die möglichen Analysemethoden für die automatisierte Datenanalyse beschränkt § 47a ASOG nicht hinreichend ((ii)). Der Eingriff wiegt auch schwer, weil der automatisierte Datenanalyse für einen Teil der Betroffenen heimlich bleibt ((iii)),

vgl. zu den Kriterien siehe oben I. 4. a) bb) (i).

(i) Art und Umfang der Daten

§ 47a Abs. 1 Satz 2 ASOG ist hinsichtlich Art und Umfang der Daten, die für die automatisierte Datenanalyse genutzt werden können, kaum beschränkt. Die Herkunft der Daten, die Menge der Daten und der Datenarten sind nicht bzw. nur kaum eingeschränkt. § 47a Abs. 2 Satz 1 ASOG ermöglicht die Einbeziehung nahezu sämtlicher polizeilich verfügbarer Datenbestände,

vgl. Berliner Beauftragte für Datenschutz und Informationsfreiheit, Stellungnahme zum Gesetzentwurf zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 2**, S. 26; vgl. zu § 25a HSOG: Bäuerle, in: BeckOK Polizei- und Ordnungsrecht Hessen, 38. Edition, Stand 1.4.2026, § 25a Rn. 52.

Durch einzelne Einschränkungen der Art und des Umfangs der Daten, die verwendet werden können, reduziert sich zwar das Eingriffsgewicht. Dies erfolgt aber nicht in einem Ausmaß, das die gebotenen Rechtfertigungsanforderungen absenken würde.

Nach § 47a Abs. 2 Satz 1 ASOG können in allen drei Tatbestandsalternativen Vorgangsdaten, Falldaten, Daten aus den polizeilichen Auskunftssystemen, Telekommunikationsdaten, Daten aus Asservaten, Daten aus dem polizeilichen Informationsaustausch weiterverarbeitet werden. Ebenfalls können in allen Varianten personenbezogene Daten aus gezielten Abfragen in Datenverbünden der Polizei (z.B. INPOL) und gesondert geführten staatlichen Registern (z.B. zentrale Verkehrsinformationssysteme, Melde- und Waffenregister) verwendet werden,

vgl. Abgh-Drs. 19/2553, S. 332 f.

Nach der Gesetzesbegründung trägt vor allem die Einbeziehung von Vorgangsdaten erheblich zur Erhöhung des Datenumfangs bei. Vorgangsdaten sind die in den Anzeigenaufnahme- und Vorgangsverwaltungsprogrammen enthaltenen Daten, mit denen das alltägliche Dienstgeschäft bewältigt wird. Hierunter fallen vor allem Anzeigen, die in gesonderter Form erfasst und gespeichert werden, sowie Vermerke. Ein Vorgang umfasst also sämtliche Unterlagen, die im Zusammenhang mit einer polizeilichen Tätigkeit über eine bestimmte Person, Sache oder einen sonstigen Gegenstand polizeilichen Handelns geführt werden,

vgl. Abgh-Drs. 19/2553, S. 332; vgl. zu § 25a HSOG Hessischer LT-Drs. 20/11235, S. 12; Müller/Schwabenbauer, in: Lisken/Denninger/Bäcker PolR-HdB, 8. Aufl. 2026, Kap. 6 Rn. 1009.

Falldaten ergeben sich aus Fallbearbeitungssystemen, die der strukturierten Bearbeitung von umfangreichen Ermittlungsverfahren dienen. In den Systemen werden die Daten zu einer Person mit einem Ereignis verknüpft, das seinerseits mit weiteren Personen, Ereignisse, Institutionen oder Sachen verknüpft wird. Damit können räumliche und sonstige Beziehungen zwischen Personen, Personengruppierungen, Institutionen, Objekten und Sachen abgebildet und über Beziehungsobjekte miteinander verknüpft werden. Zudem können

umfangreiche Daten aufgenommen werden, zu denen auch Schriftstücke, Fotos, Audio- und Videodateien gehören,

vgl. Abgh-Drs. 19/2553, S. 332; Arzt, in: Lisken/Denninger/Bäcker PolR-HdB, 8. Aufl. 2026, Kap. 6 Rn 1363.

Daten aus Einsatzleit- und Einsatzdokumentationssystemen dienen der Identifikation von polizeilichen Einsätzen, die nicht anderweitig in Vorgangsverwaltungssystemen erfasst wurden und somit für die gefahrenabwehrende Analyse unzugänglich blieben (z. B. polizeiliche Kontrollen oder verdächtige Wahrnehmungen),

Abgh-Drs. 19/2553, S. 332.

Polizeiliche Auskunftssysteme bestehen aus unterschiedlichen Datengruppen und dienen dem Nachweis und der Auskunft über Personen, die beispielsweise zur Fahndung ausgeschrieben sind, einer erkennungsdienstlichen Behandlung unterzogen wurden, inhaftiert sind bzw. waren oder in einer Kriminalakte bei einer kriminalaktenführenden Dienststelle der Polizei geführt werden. Daneben enthalten polizeiliche Auskunftssysteme die zur Fahndung ausgeschriebenen Fahrzeuge und sonstige Gegenstände, nach denen gefahndet wird,

Abgh-Drs. 19/2553, S. 332.

Telekommunikationsdaten sind die gesondert gespeicherten Datenbestände, in denen Daten aus polizeilichen Maßnahmen der Telekommunikationsüberwachung (z.B. nach §§ 26, 26a ASOG) zusammengeführt werden,

Abgh-Drs. 19/2553, S. 332.

Asservate sind amtlich in Verwahrung genommene und als Beweismittel in Frage kommende Gegenstände, soweit sie zur Aufbewahrung personenbezogener Daten dienen, wie beispielsweise Laptops, Smartphones, USB-Sticks oder Festplatten,

vgl. Abgh-Drs. 19/2553, S. 332.

Der polizeiliche Informationsaustausch betrifft den Fernschreibverkehr, die formelle elektronische Kommunikation sowie den dienstlichen E-Mail-Verkehr, soweit sie zur Übermittlung von Informationen verwendet

werden, die für die polizeiliche Aufgabenerfüllung relevant sind. Demnach beschränkt sich der Datenabgleich auf den dienstlichen E-Mail-Verkehr von Funktionspostfächern mit entsprechender Ermittlungsrelevanz,

Abgh-Drs. 19/2553, S. 332 f.

Nach § 47a Abs. 2 Satz 5 ASOG werden zwar die Vorgangsdaten Unbeteiligter – also z.B. Tatopfer und Zeug*innen – nicht in die Datenanalyse einbezogen,

vgl. zum Begriff „Unbeteiligter“ Abgh-Drs. 19/2553, S. 332.

Allerdings erfolgt in der polizeilichen Praxis keine Trennung von Vorgangsdaten Unbeteiligter und Beteiligter. Daher ist ein verlässlicher Ausschluss nicht möglich ist. Es ist zu befürchten, dass massenhaft Daten von Personen in die Analyse einfließen, die keinen Anlass für die Maßnahme gegeben haben,

vgl. Berliner Beauftragte für Datenschutz und Informationsfreiheit, Stellungnahme zum Gesetzentwurf zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 2**, S. 26.

Zudem bezieht sich diese Beschränkung nur auf Vorgangsdaten. Bei anderen Daten, die zum Teil sensiblere Informationen enthalten können, wie beispielsweise Telekommunikationsdaten, können auch die Daten Unbeteiligter in die Analyse einbezogen werden,

vgl. Bäuerle, in: BeckOK Polizei- und Ordnungsrecht Hessen, 38. Edition, Stand 1.4.2026, § 25a Rn. 57: grundrechtlich sehr relevante Datenquelle.

Aufgrund ihrer Streubreite enthalten solche Daten typischerweise eine Vielzahl personenbezogener Daten Unbeteiligter. Diese können auch rechtmäßig miterhoben werden (vgl. § 26 Abs. 1 Satz 3, § 26a Abs. 1 ASOG). Außerdem können auch Asservate, beispielsweise Datenträger wie USB-Sticks, Festplatten, Smartphones und Laptops, große Mengen personenbezogener Daten Unbeteiligter erhalten. Durch die Einbeziehung einer Vielzahl von Daten unbeteiligter Personen steigt deren Risiko, Ziel weiterer Überwachungsmaßnahmen zu werden,

vgl. BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19 –, Rn. 77.

Bei der Tatbestandsvariante des § 47a Abs. 1 Satz 2 Nr. 1 ASOG (konkrete Gefahr), können auch Nutzungs- und Verkehrsdaten weiterverarbeitet werden. Nutzungsdaten sind die in polizeilichen Datenbeständen enthaltenen personenbezogenen Informationen über die Nutzung von digitalen Diensten, die durch Telekommunikationsdiensteanbieter erhoben werden. Das umfasst insbesondere Merkmale zur Identifikation der Nutzerin oder des Nutzers, Angaben über Beginn und Ende sowie den Umfang der jeweiligen Nutzung und Angaben über die von der Nutzerin oder vom Nutzer in Anspruch genommenen digitalen Dienste,

Abgh-Drs. 19/2553, S. 332.

Nutzungsdaten ermöglichen aber weitreichende Rückschlüsse auf das Kommunikationsverhalten und damit auf persönliche Beziehungen und Lebensumstände. Ihre Einbeziehung in die automatisierte Datenanalyse erhöht das Eingriffsgewicht erheblich,

vgl. Berliner Beauftragte für Datenschutz und Informationsfreiheit, Stellungnahme zum Änderungsantrag der Fraktion der CDU und der Fraktion der SPD zur Drucksache 19/2553: Gesetz zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 7**, S. 6.

Eingriffsverstärkend ist weiter, dass für die automatisierte Datenanalyse nach § 47a Abs. 1 Satz 2 ASOG auch personenbezogene Daten einbezogen werden können, die durch besonders schwere Grundrechtseingriffe erlangt worden sind. Dabei handelt es sich um Daten, die einen sehr hohen Persönlichkeitsbezug aufweisen. Einschränkungen sieht § 47a Abs. 1 Satz 2 ASOG insoweit nicht vor,

siehe oben a) aa).

Werden Daten mit derart hohem Persönlichkeitsbezug im Rahmen des § 47a Abs. 1 Satz 2 ASOG verarbeitet, um neue Erkenntnisse zu gewinnen, ist die Wahrscheinlichkeit hoch, dass die neu gewonnen Erkenntnisse besonders private und persönlichkeitsrelevante Informationen enthalten. Insbesondere ermöglicht eine solche Verarbeitung auch die Bildung neuer Zusammenhänge und damit die

Erstellung von Persönlichkeits-, Verhaltens- und Beziehungsprofilen, die in dieser Form aus den einzelnen Ausgangsdaten nicht unmittelbar hervorgehen. Je umfassender und personenbezogener die einbezogenen Daten sind, desto weiter reicht damit das durch die Verarbeitung erzeugbare Wissen über die betroffene Person. Dies wirkt eingriffserhöhend,

vgl. BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19 –, Rn. 77.

Die Eingrenzung in § 47a Abs. 1 Satz 3 ASOG, wonach die Maßnahmen nur zulässig sind, „wenn sie nicht außer Verhältnis zur Bedeutung des aufzuklärenden Sachverhalts steht“, stellt keine hinreichende Beschränkung der Datenmenge dar. Dabei handelt es sich lediglich um einen – deklaratorischen – Hinweis auf die in jedem Fall auf Rechtsfolgenseite durchzuführende Verhältnismäßigkeitsprüfung.

Hinzu kommt, dass § 47a ASOG keine herkunftsmäßige Beschränkung enthält. Ausgeschlossen sind in der Norm weder Daten aus anderen Bundesländern oder dem Zuständigkeitsbereich des Bundes noch aus anderen Staaten,

vgl. BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19 –, Rn. 127.

Nach der Norm ist es auch zulässig, personenbezogene Daten, die Nachrichtendienste an Polizeibehörden übermittelt haben und sich nunmehr in polizeilichen Datenbeständen befinden, für die automatisierte Datenanalyse zu verwenden,

vgl. Botta, Stellungnahme zum Gesetz zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 3**, S. 13.

§ 47a ASOG enthält zudem weder eine Beschränkung auf bestimmte Datenarten noch auf die einzubeziehenden Dateiformate oder den Ausschluss biometrischer Daten,

vgl. Botta, Stellungnahme zum Gesetz zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 3**, S. 14.

Die Beschränkung des § 47a Abs. 2 Satz 3 ASOG trägt ebenfalls nicht dazu bei, dass Eingriffsgewicht wesentlich zu verringern, zumal sie durch § 47a Abs. 2 Satz 4 ASOG relativiert wird,

siehe oben a) aa).

Dasselbe gilt für § 47a Abs. 2 Satz 7 ASOG. Diese Einschränkung ist derart unbestimmt, dass sie nicht zur Reduzierung des Eingriffsgewichts beitragen kann. Nach § 47a Abs. 2 Satz 7 ASOG ist in einem Konzept der Kategorisierung und Kennzeichnung personenbezogener Daten anhand der Maßstäbe des Veranlassungszusammenhangs und der Grundrechtsrelevanz vorzusehen, welche personenbezogenen Daten in welcher Weise in eine automatisierte Anwendung zur Datenanalyse einbezogen werden dürfen. Die Entscheidung über die konkreten Rahmenbedingungen – also welche Daten genau einbezogen werden – regelt nicht der Gesetzgeber, sondern sie sind einem behördeninternen „Konzept“ vorbehalten.

Eine gesetzliche Konkretisierung wäre erforderlich, da der Gesetzgeber unter anderem mit dem Begriff des „Veranlassungszusammenhangs“ und der „Grundrechtsrelevanz“ unbestimmte Rechtsbegriffe verwendet. Angesichts des Umfangs des für die automatisierte Analyse zur Verfügung stehenden Datenpools, wäre eine gesetzgeberische Klarstellung erforderlich gewesen,

vgl. Bäuerle, in: BeckOK Polizei- und Ordnungsrecht Hessen, 38. Edition, Stand 1.4.2026, § 25a Rn. 127.

(ii) Analysemethoden

Ebenfalls erheblich eingriffserhöhend wirkt sich aus, dass § 47a Abs. 1 Satz 2 ASOG komplexe Datenanalysen ermöglicht. Die zugelassenen Methoden der Datenanalyse in § 47a ASOG sind nur geringfügig und durch den Gesetzgeber nicht hinreichend bestimmt eingeschränkt.

Die zugelassenen Analysemethoden in § 47a ASOG sind kaum begrenzt. Vielmehr hat der Gesetzgeber im Laufe des Gesetzgebungsverfahrens die Analysemethoden – anstatt sie durch gesetzliche Konkretisierung zu beschränken – sogar noch auf den Einsatz selbstlernender KI-Systeme ausgeweitet,

vgl. Änderungsantrag der Fraktion der CDU und der Fraktion der SPD zur Drucksache 19/2553, **Anlage 6**, S. 42.

Nach § 47a Abs. 1 Satz 5 ASOG lässt der Gesetzgeber den Einsatz von selbstlernenden KI-Systemen und damit hochkomplexe Verarbeitungsmethoden zu,

vgl. Botta, Stellungnahme zum Gesetz zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 3**, S. 16; Weizenbaum-Institut, Stellungnahme zur Novellierung des Allgemeinen Sicherheits- und Ordnungsgesetzes Berlin (ASOG Bln), Policy Paper #19, März 2026, S. 26.

Mit dieser bewussten Öffnung für den Einsatz von selbstlernenden KI-Systemen zielt der Gesetzgeber darauf, ein „breites Spektrum von Anbietern für Systeme der automatisierten Datenanalyse zu ermöglichen“,

vgl. Änderungsantrag der Fraktion der CDU und der Fraktion der SPD zur Drucksache 19/2553, **Anlage 6**, S. 42.

Dies stellt einen besonders schweren Eingriff dar,

vgl. Bäuerle, in: BeckOK Polizei- und Ordnungsrecht Hessen, 38. Edition, Stand 1.4.2026, § 25a Rn. 69.1.

Auf dieser Basis sind insbesondere auch komplexes Data-Mining und Risikobewertungen auf der Basis personenbezogener Daten möglich. Das Risiko beim Einsatz von selbstlernenden KI-Systemen ist, dass sich die algorithmischen Systeme im Verlauf des maschinellen Lernprozesses immer mehr von der ursprünglichen menschlichen Programmierung lösen und so maschinelle Lernprozesse und Ergebnisse der Anwendung immer schwerer nachvollziehbar werden.

Der Einsatz von selbstlernenden KI-Systemen ist bei den Tatbestandsalternativen des § 47a Abs. 1 Satz 2 Nr. 1 und Nr. 3 ASOG unter denselben Voraussetzungen möglich, wie sie für die automatisierte Datenanalyse vorgesehen sind (§ 47a Abs. 1 Satz 5 ASOG). Einzig bei der Tatbestandsalternative des § 47a Abs. 1 Satz 2 Nr. 2 ASOG bestehen nach § 47a Abs. 1 Satz 5 ASOG geringe Abweichungen. Danach wird nicht mehr auf den Straftatenkatalog des

§ 100a Abs. 2 StPO, sondern auf den des § 100b Abs. 2 ASOG verwiesen.

Aber selbst wenn KI-Systeme eingesetzt werden sollten, die nicht selbstlernend sind, können hieraus Risiken für die Nachvollziehbarkeit herrühren. Auch komplexe deterministische Systeme, deren Analysevorgänge sich nicht verändern können, bergen Risiken, da auch hier Analysevorgänge wegen ihrer Komplexität schwer nachvollziehbar sein können.

Das Eingriffsgewicht erhöht sich auch durch die Offenheit des Suchvorgangs. Zwar sieht § 47a Abs. 1 Satz 4 ASOG vor, dass die automatisierte Anwendung zur Auswertung vorhandener Daten anhand von Suchbegriffen erfolgt, die sich aus einem konkreten Sachverhalt, bezogen auf einen Anlass im Sinne des § 47a Abs. 1 Satz 2 ASOG ergeben. Die Suchbegriffe können aber derart allgemein (z.B. Messer, Auto) sein, dass dies einer offenen Suche gleichkommt.

Daneben ist auch die automatisierte Datenanalyse für „statistische Zwecke“ zulässig. Unklar ist noch, welchen Anwendungsbereich die Analyse für statistische Zwecke hat,

vgl. BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19 –, Rn. 93; Berliner Beauftragte für Datenschutz und Informationsfreiheit, Stellungnahme zum Gesetzentwurf zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 2**, S. 24.

Die Beschränkung in § 47a Abs. 1 Satz 7 ASOG, dass nur mit den Suchparametern übereinstimmende Daten (Treffer) angezeigt werden, reduziert das Eingriffsgewicht nicht wesentlich. Denn es sind weiterhin offene Suchen und Suchanfragen möglich, die sich zum Beispiel auf statistische Auffälligkeiten in der Datenmenge richten. Auch ist die Anzahl der Suchanfragen und Abgleichsschritte nicht von vornherein begrenzt, sodass komplexe Analysen mit immer wieder aufeinander aufbauenden Suchanfragen möglich sind.

Die Art der möglichen Suchergebnisse wirkt sich eingriffsverstärkend aus. Die Einschränkungen, die § 47a ASOG vorsieht, reduzieren das Eingriffsgewicht nicht wesentlich. § 47a Abs. 1 Satz 8 ASOG sieht zwar

vor, dass automatisierte Entscheidungsfindungen unzulässig sind. Hierdurch soll gewährleistet werden, dass jede Entscheidung einem Menschen vorbehalten bleibt,

Abgh-Drs. 19/2553, S. 331.

Nach dem Wortlaut der Norm genügt aber schon eine minimale menschliche Mitwirkung, dass der automatisierte Datenabgleich zulässig ist. Es ist vom Wortlaut auch grundsätzlich erfasst, dass eine bloße formale Nachbereitung erfolgen könnte. Es könnte auch den Anforderungen genügen, wenn der überprüfenden Person kein Entscheidungsspielraum zukommt, solange die Entscheidung am Ende von einem Menschen getroffen wird. Hinzu kommt die Gefahr des sogenannten Automation Bias,

vgl. Botta, Stellungnahme zum Gesetz zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 3**, S. 17 sowie oben I. 4. a) bb) (ii).

§ 47a Abs. 1 Satz 8 ASOG schließt zwar die automatisierte Sachverhaltsbewertung aus. Hiernach sollen laut Gesetzesbegründung insbesondere personenbezogene Gefährlichkeitsaussagen im Sinne eines „predictive policing“ unzulässig sein,

vgl. Abgh-Drs. 19/2553, S. 331.

Es bleibt jedoch unklar, was unter dem Begriff der „automatisierten Sachverhaltsbewertung“ zu fassen ist. Zudem bleibt unklar, ob und inwieweit die unterstützende Sachverhaltsbewertung durch automatisierte Datenanalyse zulässig sein soll. Diese ist nach dem Wortlaut von § 47a Abs. 1 Satz 8 ASOG nicht ausgeschlossen. Es würde auch nur eine minimale menschliche Beteiligung genügen, um die Anforderungen des § 47a Abs. 1 Satz 8 ASOG einzuhalten.

Das Eingriffsgewicht erhöht sich auch dadurch, dass die zugelassenen Analysemethoden diskriminierende Entscheidungen ermöglichen. Daran vermag auch § 47a Abs. 1 Satz 6 ASOG nichts zu ändern. Danach ist durch geeignete Maßnahmen sicherzustellen, dass bei der automatisierten Datenanalyse diskriminierende Algorithmen weder herausgebildet noch verwendet werden. Diese Vorkehrung ist aber

derart unbestimmt, dass sie nicht zu einer Reduzierung des Eingriffsgewichts beiträgt. Die technisch-organisatorischen Vorkehrungen hätte der Gesetzgeber zumindest in Grundzügen regeln müssen. Dies gilt umso mehr, als dass § 47a Abs. 1 Satz 5 ASOG den Einsatz selbstlernender KI-Systeme zulässt.

Der Gesetzgeber hat auch keine Vorkehrungen zur Erkennung von Fehlern getroffen, die das Eingriffsgewicht abmildern,

siehe dazu näher unten dd).

Die Eingriffsintensität steigt auch dadurch, dass der Gesetzgeber keine Beschränkungen vorgesehen hat, woher die Systeme zur automatisierten Datenanalyse stammen können. Es ist gerade zu erwarten, dass wegen der Komplexität dieser Systeme auf den Sachverstand und bereits entwickelte Systeme von Dritten zurückgegriffen wird. Wegen der Komplexität der Systeme zur automatisierten Datenanalyse steigt das Risiko, die staatliche Kontrolle über deren Anwendung zu verlieren.

§ 47a ASOG schließt nicht aus, dass auf Systeme von privaten Dritten wie Palantir zurückgegriffen wird,

siehe oben 2.

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. Manipulation und mögliche Hintertüren und damit das Risiko von Leaks und unbefugten Zugriffen auf polizeiliche Daten können nie, auch nicht durch vertragliche Vereinbarungen vollständig ausgeschlossen werden. Wird Software privater Akteure oder anderer Staaten eingesetzt, besteht zudem eine Gefahr unbemerkter Manipulation oder des unbemerkten Zugriffs auf Daten durch Dritte,

vgl. BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19, 1 BvR 2634/20 –, Rn. 100.

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, etwa wenn zur Wartung Personal des privaten Unternehmens innerhalb der polizeilichen Infrastruktur mit Zugang zu den polizeilichen Servern eingesetzt wird. 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. Andere Normen des ASOG – z.B. § 42d Abs. 3 Satz 3 ASOG – sehen vor diesem Hintergrund Beschränkungen vor, wo der Sitz des Dritten liegen darf. Eine solche Einschränkung fehlt indes bei der – im Vergleich zum KI-Training eingriffsintensiveren – automatisierten Datenanalyse.

Ebenso besteht beim Einsatz der Software privater Anbieter*innen die Gefahr, dass Algorithmen und Ergebnisse intransparent bleiben 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,

vgl. BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19, 1 BvR 2634/20 –, Rn. 100.

Das Eingriffsgewicht sinkt auch nicht maßgeblich durch § 47a Abs. 3 Satz 1 bis 5 ASOG. § 47a Abs. 3 Satz 1 ASOG sieht eine Zugriffsbeschränkung auf die automatisierte Datenanalyse für ausgewählte und geschulte Polizeikräfte vor. Allerdings verringert die Zahl der Zugriffsberechtigten nicht wesentlich das Eingriffsgewicht. Vielmehr wird dies nur erreicht, wenn durch die Zugriffsbeschränkungen

weniger Auswertungs- und Analysevorgänge in Gang gesetzt und weniger Daten verarbeitet werden,

vgl. Bäuerle, in: BeckOK Polizei- und Ordnungsrecht Hessen, 38. Edition, Stand 1.4.2026, § 25a Rn. 68.

Nach § 47a Abs. 3 Satz 3 ASOG sind durch organisatorische und technische Maßnahmen die Zugriffsmöglichkeiten der eingesetzten Polizeikräfte auf das erforderliche Maß zu begrenzen. Es ist jedoch nicht ansatzweise nachvollziehbar, welche Daten für welche geschulten Polizeikräfte erforderlich sind. Dafür gibt das Gesetz keine Kriterien vor.

Dies gilt ebenso für die Einschränkung des § 47a Abs. 3 Satz 4 ASOG. Auch hier ist nicht ersichtlich, wie das „erforderliche Maß“ für die Begrenzungen der Zugriffsrechte ausgestaltet ist. Auch hat der Gesetzgeber nicht konkretisiert, ab wann der Zugriff auf personenbezogene Daten „unverzichtbar“ im Sinne von § 47a Abs. 3 Satz 5 ASOG ist. Zwar erscheint es möglich, dafür Regelungen in einer Verwaltungsvorschrift zu treffen. Da die Anforderungen an die Regelungsdichte besonders hoch sind, hätte der Gesetzgeber nach dem Wesentlichkeitsgrundsatz hier aber zumindest spezifische Angaben zum Inhalt einer Verwaltungsvorschrift im Normtext selbst machen müssen, um eine beschränkende Wirkung wirksam zu erzielen. Dem genügt § 47a Abs. 6 Satz 1 ASOG nicht. Danach bestimmt das Nähere zu § 47a Abs. 2 bis 4 ASOG eine zu veröffentlichende Verwaltungsvorschrift. Es fehlt jedoch an einer Konkretisierung dafür, was „das Nähere“ im Sinne des § 47a Abs. 6 ASOG sein soll. Selbst beim weniger eingriffsintensiven KI-Training hat der Gesetzgeber in § 42d Abs. 4 Satz 1 ASOG den Inhalt einer Verwaltungsvorschrift konkretisiert. Auch die „Vorbildregelung“ in § 25a HSOG sieht in dessen Abs. 3 deutlich detailliertere Vorgaben vor.

(iii) Heimlichkeit

Die Eingriffsintensität erhöht sich auch dadurch, dass die automatisierte Datenanalyse zumindest für die meisten Personen heimlich ist und auch nach Abschluss der Maßnahme heimlich bleibt.

Nach § 47a Abs. 3 Satz 6 ASOG sind Personen, deren personenbezogene Daten nach § 47a Abs. 1 ASOG weiterverarbeitet wurden und gegen die anschließend weitere Maßnahmen nach diesem

Gesetz getroffen wurden, nach Abschluss der Folgemaßnahmen gemäß § 42 BlnDSG über die Datenverarbeitung zu benachrichtigen.

Für Personen, gegen die keine weitere Maßnahmen getroffen wurden, bleibt die automatisierte Datenanalyse geheim,

vgl. Berliner Beauftragte für Datenschutz und Informationsfreiheit, Stellungnahme zum Änderungsantrag der Fraktion der CDU und der Fraktion der SPD zur Drucksache 19/2553: Gesetz zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 7**, S. 7.

Auch die Benachrichtigungspflicht nach § 27d ASOG greift nicht, da diese sich nicht auf § 47a ASOG bezieht.

bb) Keine ausreichenden Voraussetzungen

Der mit § 47a Abs. 1 Satz 2 ASOG verbundene Eingriff ist nicht an hinreichende Eingriffsvoraussetzungen geknüpft.

Ermöglicht die automatisierte Anwendung einen nach den genannten Kriterien schwerwiegenden Eingriff in die informationelle Selbstbestimmung der Betroffenen, ist dies nur unter den engen Voraussetzungen zu rechtfertigen, wie sie allgemein für eingriffsintensive heimliche Überwachungsmaßnahmen gelten,

BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19 –, Rn. 104; siehe oben II. 4. b).

Solche Maßnahmen sind nur zum Schutz besonders gewichtiger Rechtsgüter zulässig. Zu den besonders gewichtigen Rechtsgütern zählen vor allem Leib, Leben und Freiheit der Person sowie Bestand oder Sicherheit des Bundes oder eines Landes. Vergleichbares Gewicht entfalten kann der Schutz von Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, sofern darunter einem engen Verständnis folgend etwa wesentliche Infrastruktureinrichtungen oder sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen gefasst werden. Auch kann der Gesetzgeber darauf verzichten, das erforderliche Rechtsgut unmittelbar zu benennen und stattdessen an entsprechende Straftaten anknüpfen, deren Verhütung mit der Befugnis bezweckt ist,

BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19 –, Rn. 105;
zum Rechtsgüterschutz siehe auch schon oben II. 4. b) aa).

Die Eingriffsschwelle ist in der Regel die hinreichend konkretisierte Gefahr. Dies setzt voraus, dass zumindest tatsächliche Anhaltspunkte für die Entstehung einer konkreten Gefahr für die Schutzgüter bestehen.

BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19 –, Rn. 106.

Sofern die Gefahr für ein überragend wichtiges Rechtsgut besteht, reicht es aus, wenn sich der zum Schaden führende Kausalverlauf noch nicht mit hinreichender Wahrscheinlichkeit vorhersehen lässt, sofern bereits bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für dieses überragend wichtige Rechtsgut hinweisen,

vgl. BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19 –, Rn. 106.

Für eine konkretisierte Gefahr bedarf es zweier Voraussetzungen: Es bedarf bestimmte Tatsachen, die – erstens – den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen und – zweitens – auch den Schluss darauf zulassen, 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,

vgl. BVerfGE 165, 363 <410 f. Rn. 106 m.w.N.>.

Die Voraussetzungen des § 47a Abs. 1 Satz 2 Nr. 2 ASOG genügt den verfassungsrechtlichen Anforderungen nicht, die angesichts der Schwere des Eingriffs erforderlich gewesen wären.

Die Norm genügt weder den Anforderungen an den Rechtsgüterschutz ((i)), noch denen an die Eingriffsschwelle ((ii)). Zudem enthält sie eine unzulässige dynamische Verweisung ((iii)). Alles gilt ebenfalls für den insoweit korrespondierenden § 47a Abs. 1 Satz 5 ASOG ((iv)).

(i) Rechtsgüterschutz

Indem § 47a Abs. 1 Satz 2 Nr. 2 lit. b) ASOG auf § 100a Abs. 2 StPO verweist, dient die Norm nicht nur dem Schutz besonders gewichtiger Rechtsgüter. Die von § 100a Abs. 2 StPO erfassten Straftatbestände

dienen nicht durchgängig dem Schutz besonders gewichtiger Rechtsgüter. Auch gemessen am Strafraumen handelt es sich nicht durchgängig um besonders schwere Straftaten.

§ 100a Abs. 2 StPO enthält eine Vielzahl von Delikten, die primär das Vermögen, Eigentum oder sonstige nicht besonders gewichtige Rechtsgüter schützen. Zu nennen sind beispielhaft das Verbreiten von Propagandamitteln verfassungswidriger Organisationen (§ 86 StGB), Geldfälschung (§ 146 Abs. 1 StGB), Banden- und Wohnungseinbruchsdiebstahl (§ 244 Abs. 1 Nr. 2 StGB) und Verleitung zur missbräuchlichen Asylantragsstellung (§ 84 Abs. 3 AsylG).

Damit öffnet die Ermächtigungsgrundlage den Rechtsgüterschutz in verfassungswidriger Weise „nach unten“,

vgl. Botta, Stellungnahme zum Gesetz zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 3**, S. 19; Bäuerle, in: BeckOK Polizei- und Ordnungsrecht Hessen, 38. Edition, Stand 1.4.2026, § 25a Rn. 40 f.

Aber auch ohne diese rechtsgutsbezogene Betrachtung handelt es sich nicht um besonders schwere Straftaten.

§ 100a Abs. 2 StPO enthält zahlreiche Tatbestände, die lediglich eine Höchstfreiheitsstrafe von drei Jahren oder weniger vorsehen und damit dem einfachen Kriminalitätsbereich zuzuordnen sind. Hierzu zählen folgende Tatbestände: § 85 Abs. 2 StGB, § 86 Absätze 1 und 2 StGB, § 97 Abs. 2 StGB, § 97b Abs. 1 Satz 1 in Verbindung mit § 97 Abs. 2 StGB, § 109g Abs. 1 in Verbindung mit Abs. 4 Satz 1 StGB, § 109g Abs. 2 StGB, § 129 Abs. 1 Satz 2 StGB, § 129 Abs. 1 Satz 2 in Verbindung mit § 129b StGB, § 130 Absätze 2, 4 und 5 StGB, § 310 Abs. 1 Nr. 4 in Verbindung mit § 309 Abs. 6 StGB, § 313 Abs. 2 in Verbindung mit § 308 Abs. 6 StGB, § 17 Abs. 5 AWG, § 18 Abs. 5a AWG, § 30b BtMG in Verbindung mit § 129 Abs. 1 Satz 2 StGB, § 30b BtMG in Verbindung mit § 129 Abs. 1 Satz 2 in Verbindung mit § 129b StGB,

siehe BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025 – 1 BvR 180/23 –, Rn. 215.

Soweit einzelne der in § 100a Abs. 2 StPO genannten Straftatbestände eine Höchstfreiheitsstrafe von fünf Jahren vorsehen, handelt es sich ebenfalls nicht durchgängig um besonders schwere Straftaten. Erforderlich wäre insoweit, dass 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,

BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025 – 1 BvR 180/23 –, Rn. 210.

Auch unter Anwendung dieses Maßstabs genügt § 100a Abs. 2 StPO den verfassungsrechtlichen Anforderungen nicht,

offenlassend BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025 – 1 BvR 180/23 –, Rn. 217.

Dies ergibt sich daraus, dass § 100a Abs. 2 StPO umfänglich, teils ausdrücklich, auf minder schwere Fälle verweist, deren Einstufung als besonders schwere Straftaten weder ihrem Strafmaß nach indiziert ist noch im Tatbestand der Norm einen den Vorgaben entsprechenden objektivierten Ausdruck findet,

vgl. oben II. 4. b. aa) zum engeren § 100b Abs. 2 StPO.

(ii) Eingriffsschwelle

Auch die Eingriffsschwelle in § 47a Abs. 1 Satz 2 Nr. 2 ASOG genügt nicht den verfassungsrechtlichen Anforderungen.

Das gilt zunächst, soweit § 47a Abs. 1 Satz 2 Nr. 2 lit. b) ASOG auf Vorfelddelikte verweist, ohne hinreichend normenklar eine konkretisierte Gefahr für ein besonders gewichtiges Rechtsgut zu verlangen,

siehe oben II. 4. b) bb).

§ 47a Abs. 1 Satz 2 Nr. 2 ASOG verankert zudem nur eine Voraussetzung der konkretisierten Gefahr. Nach dieser Norm ist eine automatisierte Datenanalyse möglich, wenn „tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass innerhalb eines übersehbaren Zeitraumes auf eine zumindest ihrer Art nach konkretisierte Weise eine terroristische Straftat oder eine in § 100a

Absatz 2 der Strafprozessordnung genannte und voraussichtlich auch im Einzelfall schwerwiegende Straftat begangen werden soll und die Maßnahme zur Verhütung dieser Straftat erforderlich ist“.

Es fehlt an dem individualisierenden Teil der Regelung, nämlich dass Tatsachen den Schluss darauf zulassen, dass bestimmte Personen an den genannten Straftaten beteiligt sein werden, über deren Identität zumindest so viel bekannt ist, dass die staatliche Maßnahme gezielt gegen sie eingesetzt und weitgehend auf sie beschränkt werden kann,

vgl. Botta, Stellungnahme zum Gesetz zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 3**, S. 18; Martini/Botta, DÖV 2025, 1033 (1041).

Auf Grundlage der Regelung des § 47a Abs. 1 Satz 2 Nr. 2 ASOG könnten auch allgemeine Informationen über Vorbereitungshandlungen zum Anlass für automatisierte Datenanalysen genommen werden, beispielsweise über die Lieferung von gefährlichen Chemikalien, Waffen oder explosiven Stoffen an einen eingegrenzten Ort. Es könnte danach eine automatisierte Datenanalyse über Personen durchgeführt werden, die individuell keinen Anlass für eine Beteiligung an einer schwerwiegenden Straftat gegeben haben. Vielmehr könnte die Datenanalyse beispielsweise durchgeführt werden, allein weil die Person einem bestimmten Profil entspricht oder sich in räumlicher Nähe zum Lieferort aufhält.

Eine Störerrichtung der Maßnahme ist gerade nicht gewollt. Der Einsatz der automatisierten Datenanalyse soll vielmehr personenoffen möglich sein. Dies zeigt der Vergleich zu § 47a Abs. 1 Satz 2 Nr. 3 ASOG. Diese Tatbestandsalternative nimmt Bezug auf das individuelle Verhalten einer Person.

(iii) Unzulässiger dynamischer Verweis

§ 47a Abs. 1 Satz 2 Nr. 2 ASOG genügt zudem nicht den verfassungsrechtlichen Anforderungen, weil die Norm eine unzulässige dynamische Verweisung auf den unzureichenden Straftatenkatalog des § 100a Abs. 2 StPO enthält. Dies widerspricht den verfassungsrechtlichen Anforderungen an Bestimmtheit und Normenklarheit,

siehe dazu bereits oben II. 4. b) cc).

Der gesetzgeberischen Begründung ist nicht zu entnehmen, ob auf § 100a Abs. 2 ASOG nur in seiner aktuellen bundesgesetzlichen Fassung verwiesen werden soll,

vgl. Abgh-Drs. 19/2553, S. 330.

Vor diesem Hintergrund handelt es sich um eine dynamische Verweisung. Der Gesetzgeber übernimmt mit dieser Regelungstechnik in unzulässiger Weise eine fremde Abwägungsentscheidung des Bundesgesetzgebers. Da der Bund diese Norm jederzeit verändern kann, kann der Gesetzgeber deren Gewicht nicht kennen und daher auch nicht in seine Abwägung einstellen,

siehe oben II. 4. b) cc) und BVerfGE 162, 1 <170 Rn. 386> zu einem dynamischen Verweis auf § 100b Abs. 2 StPO in einer sicherheitsrechtlichen Ermächtigungsgrundlage.

(iv) § 47a Abs. 1 Satz 5 ASOG

Das oben Gesagte gilt ebenfalls für § 47a Abs. 1 Satz 5 ASOG. Diese Norm stellt leicht verschärfte Anforderungen an den Einsatz selbstlernender Systeme,

siehe oben aa) (ii).

Danach ist die Nutzung selbstlernender Systeme zulässig, wenn „tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass innerhalb eines übersehbaren Zeitraumes auf eine zumindest ihrer Art nach konkretisierte Weise eine terroristische Straftat oder eine in § 100b Absatz 2 der Strafprozessordnung genannte und voraussichtlich auch im Einzelfall besonders schwerwiegende Straftat begangen werden soll und die Maßnahme zur Verhütung dieser Straftat erforderlich ist“.

Auch diese Norm sieht keine Personenkreiseingrenzung vor,

siehe oben (ii).

Weiterhin erfasst § 100b Abs. 2 StPO Straftaten, die den Rechtsgüterschutz in verfassungswidriger Weise nach unten öffnen,

siehe oben II. 4. b) aa).

Ebenso ist die dynamische Verweisung unzulässig,

siehe oben II. 4. b) cc).

cc) Unzureichende Kennzeichnungspflicht

Nach § 47a Abs. 2 Satz 6 ASOG gilt zwar die Kennzeichnungspflicht nach § 42b ASOG. Diese wird aber durch weitgehende Ausnahmeregelungen des § 42b Abs. 4 Satz 1 ASOG erheblich abgeschwächt,

siehe oben IV. und Botta, Stellungnahme zum Gesetz zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 3**, S. 12.

Der Gesetzgeber hätte sicherstellen müssen, dass nur gekennzeichnete Daten in die automatisierte Datenanalyse einfließen können. Nur so ist es möglich, dass die Voraussetzungen der Zweckbindung und hypothetischen Datenneuerhebung eingehalten werden,

Berliner Beauftragte für Datenschutz und Informationsfreiheit, Stellungnahme zum Gesetzentwurf zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 2**, S. 20.

Dies hat er für das – im Vergleich zur automatisierten Datenanalyse sogar weniger eingriffsintensive – KI-Training angeordnet, § 42b Abs. 4 Satz 2 ASOG.

Die Ausnahmen von der Kennzeichnung können insbesondere zu Lasten von Unbeteiligten gehen. In der Praxis ist schon unklar, wie die Kategorisierung, Identifizierung, Kennzeichnung und Abtrennung der Datensätze unbeteiligter Personen erfolgen kann,

vgl. Berliner Beauftragte für Datenschutz und Informationsfreiheit, Stellungnahme zum Gesetzentwurf zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 2**, S. 26.

dd) Fehlende Vorkehrungen gegen Fehler, Diskriminierung und Datenmissbrauch

Bei komplexen Formen der Datenanalyse insbesondere mittels künstlicher Intelligenz sind zudem spezifische und normenklare

Vorkehrungen gegen Fehler, Diskriminierung und Datenmissbrauch erforderlich,

siehe zum Maßstab oben I. 4. b) ee).

Dies kann etwa auch gesetzliche Regelungen zu einem staatlichen Monitoring der Entwicklung der eingesetzten Software erfordern,

BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19, 1 BvR 2634/20 –, Rn. 109.

Solche Vorgaben lassen sich § 47a ASOG nicht entnehmen.

Insbesondere fehlt es an einem staatlichen Monitoring der eingesetzten Software, obwohl der Einsatz von Systemen privater Anbieter nicht ausgeschlossen ist,

vgl. Bäuerle, in: BeckOK Polizei- und Ordnungsrecht Hessen, 38. Edition, Stand 1.4.2026, § 25a Rn. 83.

§ 47a Abs. 4 ASOG enthält zwar eine Befugnis zur Verarbeitung personenbezogener Daten, um die automatisierte Datenanalyse zu testen. Eine Pflicht zur Testung wird jedoch nicht statuiert.

Auch die Regelung des § 47a Abs. 1 Satz 6 ASOG, nach der durch geeignete Maßnahmen sicherzustellen ist, dass bei der automatisierten Datenanalyse diskriminierende Algorithmen weder herausgebildet noch verwendet werden, ist vor dem Hintergrund des Eingriffsgewichts und des möglichen Einsatzes selbstlernender KI-Systeme unzureichend. Es bleibt unklar, wie genau dies sicherzustellen ist,

vgl. oben I. 4. b) ee) und Bäuerle, in: BeckOK PolR Hessen, 39. Ed. 1.7.2026, HSOG § 25a Rn. 138; Arzt, in: BeckOK PolR NRW/Arzt, 34. Ed. 15.4.2026, PolG NRW § 23 Rn. 82.

§ 47a ASOG sieht auch keine hinreichenden Vorkehrungen gegen den Schutz vor Missbrauch vor, wenn auf ein privates System zur automatisierten Datenanalyse zurückgegriffen wird. Diesbezüglich fehlt es gänzlich an Schutzvorkehrungen, wie sie zum Beispiel § 42d Abs. 3 ASOG vorsieht.

ee) Keine ausreichenden Kontrollen

Auch die behördlichen Kontrollmechanismen, die § 47a ASOG vorsieht, genügen nicht den verfassungsrechtlichen Anforderungen. Da der Eingriff, der mit § 47a Abs. 1 Satz 2 ASOG einhergeht, auch heimlich bleiben kann,

siehe oben aa) (iii),

hätte der Gesetzgeber eine strengere Kontrolle vorsehen müssen.

§ 47a Abs. 3 Satz 7 ASOG sieht zwar vor, dass die oder der behördliche Datenschutzbeauftragte spätestens alle zwei Jahre stichprobenartige Kontrollen durchführt. Ein Intervall von zwei Jahren ist für eine derart eingriffsintensive Maßnahme unzureichend. Dies gilt insbesondere wegen der zugelassenen Nutzung von selbstlernenden KI-Systemen. Deren Entscheidungsmuster können sich kurzfristig verändern,

vgl. Berliner Beauftragte für Datenschutz und Informationsfreiheit, Stellungnahme zum Änderungsantrag der Fraktion der CDU und der Fraktion der SPD zur Drucksache 19/2553: Gesetz zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin, **Anlage 7**, S. 7.

Zudem fehlt es an einer ausreichenden Kontrollen durch die Berliner Beauftragte für Datenschutz und Informationsfreiheit. § 51b Satz 1 Nr. 1 ASOG sieht zwar vor, dass die oder der Berliner Beauftragte für Datenschutz und Informationsfreiheit spätestens alle zwei Jahre stichprobenartige Kontrollen bezüglich der nach § 47a Abs. 3 Satz 5 ASOG zu protokollierenden Maßnahmen durchführt. Ein Intervall von zwei Jahren ist aber auch für diese Kontrolle wegen des möglichen Einsatzes selbstlernender KI-Systeme unzureichend.

David Werdermann
Rechtsanwalt