Deutsches Forschungsinstitut
für öffentliche Verwaltung
German Research Institute
for Public Administration

FÖV / Postfach 14 09 / 67324 Speyer

An den Ausschuss für Inneres und Sport
des Landtages von Sachsen-Anhalt

Dr. Jonas Botta
Forschungsreferent
botta@foev-speyer.de

08.04.2025

Stellungnahme zum Entwurf eines Elften Gesetzes zur Änderung des Gesetzes über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt

Sehr geehrte Damen und Herren Abgeordnete,

anbei darf ich Ihnen meine Stellungnahme zum o.g. Gesetzentwurf übersenden. Ich hoffe, die aufgezeigten Punkte können Ihnen bei Ihrer Entscheidungsfindung behilflich sein.

Mit freundlichen Grüßen

Jonas Botta

DR. JONAS BOTTA

Stellungnahme zum Entwurf eines Elften Gesetzes zur Änderung des Gesetzes über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt

(LT-Drs. 8/5018)

A. Überblick

Der Gesetzentwurf zur Änderung des Gesetzes über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt (SOG LSA) sieht vor, der Polizei eine Vielzahl neuer Befugnisse zu verleihen. Die nachfolgende Stellungnahme konzentriert sich auf zwei Regelungsvorschläge, die von besonderer Brisanz sind: die Ermächtigungsgrundlagen zur **automatisierten Kennzeichenerfassung (§ 16b SOG LSA)** und zur **automatisierten Datenanalyse (§ 30a SOG LSA)**. Beide Befugnisse sind nicht nur äußerst grundrechtssensibel, sie betreffen auch eine große Personenanzahl – sowohl aus Sachsen-Anhalt als auch aus dem gesamten Bundesgebiet (und darüber hinaus). Es ist daher positiv hervorzuheben, dass sich die Landesregierung ersichtlich darum bemüht hat, bei der Erarbeitung der Normen die einschlägige Rechtsprechung des BVerfG möglichst umfassend zu berücksichtigen. Während ihr dieses Unterfangen bei der automatisierten Kennzeichenerfassung weitgehend gelungen ist, steht ihr Entwurf einer Ermächtigungsgrundlage für die automatisierte Datenanalyse überwiegend auf verfassungsrechtlich tönernen Füßen.

Sollte der Landtag nicht die erforderlichen Korrekturen vornehmen, schwebte über der Modernisierung der Gefahrenabwehr dauerhaft das Damoklesschwert der **Verfassungswidrigkeit**. Dann fiele es höchstwahrscheinlich dem BVerfG zu, nachträglich für einen verfassungsgemäßen Zustand zu sorgen, was nicht nur die Polizeiarbeit erschwerte, da bereits etablierte Verfahren geändert werden müssten, sondern vor allem auch das gesellschaftliche **Vertrauen in die Polizei und den Rechtsstaat** insgesamt beschädigte.

B. Automatisierte Kennzeichenerfassung (§ 16b SOG LSA)

Der vorgeschlagene § 16b SOG LSA soll der Polizei zukünftig den Einsatz automatisierter Kfz-Kennzeichenerkennungssysteme erlauben.

I. Grundrechtseingriff

Das BVerfG hat bereits wiederholt zu Kfz-Kennzeichenkontrollen entschieden (zuletzt 2018). Nach seiner neuen Rechtsprechungslinie begründet eine automatisierte Kfz-Kennzeichenkontrolle

Eingriffe in das Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) aller Personen, deren Kennzeichen in die Kontrolle einbezogen werden, auch wenn das Ergebnis zu einem „Nichttreffer“ führt und die Daten sogleich gelöscht werden.[1] Insbesondere entfällt der grundrechtliche Schutz nicht schon deshalb, weil das Kfz-Kennzeichen öffentlich einsehbar ist.[2] Auch wenn sich der Einzelne in die Öffentlichkeit begibt, schützt die informationelle Selbstbestimmung dessen Interesse, dass die damit verbundenen personenbezogenen Informationen nicht im Zuge automatisierter Informationserhebung zur Speicherung mit der Möglichkeit der Weiterverwertung erfasst werden.[3] Maßgeblich ist allein, dass sich **das Kennzeichen eindeutig einer bestimmten Person zuordnen lässt** und damit personenbezogene Informationen vermitteln kann.[4] Die Kontrolle erfasst Kfz-Kennzeichen sowie Ort, Datum, Uhrzeit und Fahrtrichtung des Kraftfahrzeugs (§ 16b Abs. 1 S. 1 aE SOG LSA); diese Informationen können mittels einer Halterabfrage einer bestimmten Person zugeordnet werden. Ein erster Eingriff liegt grundsätzlich in der Erfassung personenbezogener Daten.[5] Ein weiterer Eingriff liegt in dem Abgleich der Daten sowie in der folgenden Verwendung der gefilterten Daten.[6]

II. Rechtfertigung

Grundrechtseingriffe durch eine automatisierte Kfz-Kennzeichenkontrolle lassen sich grundsätzlich rechtfertigen.

---

[1] BVerfGE 150, 244 (263 ff.); 150, 309 (330 ff.); Abweichung von BVerfGE 120, 378.

[2] BVerfGE 150, 244 (264 f.).

[3] BVerfGE 120, 378 (399); 150, 244 (265).

[4] BVerfGE 120, 378 (400 f.); 150, 244 (265); Brenner, DAR 2019, 241 (241); vgl. BVerfGE 65, 1 (42).

[5] 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 (BVerfGE 150, 244 (266)).

[6] BVerfGE 150, 244 (266).

1. Formelle Verfassungsmäßigkeit

Gegen die formelle Verfassungsmäßigkeit von § 16b SOG LSA bestehen keine Einwände. Zwar fällt der Grenzschutz in die ausschließliche Gesetzgebungskompetenz des Bundes (Art. 73 Abs. 1 Nr. 5 GG) und dient die polizeirechtliche Norm der vorbeugenden Bekämpfung der grenzüberschreitenden Kriminalität. Aber dass mit Kennzeichenkontrollen Zwecke verfolgt werden, die einen Grenzbezug haben, macht sie nicht ohne Weiteres zu Regelungen des Grenzschutzes. Vielmehr handelt es sich um **Regelungen zur Gefahrenabwehr**, die zwar an die Offenheit der Grenzen und damit einhergehende Gefahren anknüpfen, jedoch nicht unmittelbar dem Schutz der Bundesgrenze dienen.[7] Dies gilt insbesondere auch für die Bekämpfung der grenzüberschreitenden Kriminalität. Denn hierunter sind nicht Verstöße speziell gegen Strafvorschriften zum Grenzschutz selbst zu verstehen, sondern allgemein Straftaten, die die tatsächlichen und rechtlichen Besonderheiten der Grenzsituation oder Grenznähe, insbesondere die Erschwerungen grenzüberschreitender Fahndung und Strafverfolgung, ausnutzen.[8] Infolge seines gefahrenabwehrrechtlichen Regelungszweckes – dem die vorbeugende Bekämpfung von Straftaten ebenfalls dient[9] – kollidiert § 16b SOG LSA auch nicht mit Art. 74 Abs. 1 Nr. 1 GG, auf dessen Grundlage der Bundesgesetzgeber § 163g StPO[10] (Automatische Kennzeichenerfassung) erlassen hat. Der Regelungsbefugnis des Landes stehen auch keine anderen Kompetenztitel des Bundes entgegen. Insbesondere handelt es sich bei § 16b SOG LSA nicht um eine Regelung des Straßenverkehrs i.S.d. Art. 74 Abs. 1 Nr. 22 GG.[11]

2. Materielle Verfassungsmäßigkeit

Die materielle Verfassungsmäßigkeit des vorgeschlagenen § 16b SOG LSA bemisst sich insbesondere nach dem **Verhältnismäßigkeitsgrundsatz**. Seine Ermächtigungen zur automatisierten

---

[7] BVerfGE 150, 244 (271).

[8] BVerfGE 150, 244 (271); vgl. SächsVerfGH, Urt. v. 10.7.2003, Az.: Vf. 43-II-00, juris, Rn. 187 f. = BeckRS 2003, 12595.

[9] BVerfGE 113, 348 (368).

[10] Dazu z.B. Roggan, NStZ 2022, 19 (19 ff.).

[11] BVerfGE 150, 309 (335).

Kfz-Kennzeichenerfassung und zum Datenabgleich müssen einen legitimen Zweck verfolgen, zur Erreichung des Zwecks geeignet, erforderlich und angemessen sein.[12] Dabei müssen sie zugleich den Grundsätzen der Normenklarheit und Bestimmtheit genügen.

a) Legitimer Zweck

§ 16b SOG LSA dient der vorbeugenden Bekämpfung der grenzüberschreitenden Kriminalität, der Verhütung von Straftaten sowie der Abwehr erheblicher Gefahren und damit legitimen Zwecken.[13]

b) Geeignetheit und Erforderlichkeit

Für diese Zwecke sind automatisierte Kfz-Kennzeichenkontrollen auch förderlich, d.h. geeignet. Dass der Abgleich ausschließlich Kfz-Kennzeichen betrifft, sodass Treffer **nur indirekt** den Fahrzeughalter identifizieren (der zudem nicht zwangsläufig die gesuchte Person selbst sein muss), ändert nichts an der Geeignetheit der Maßnahme. Denn die Wahrscheinlichkeit, auf diesem Weg die i.R.d. Kontrolle gesuchten Personen oder Gegenstände zu finden, wird dadurch zumindest erhöht.[14] Für die Erreichung der Zwecke des § 16b SOG LSA sind automatisierte Kennzeichenkontrollen mangels milderer, gleich geeigneter Mittel auch erforderlich.[15]

c) Angemessenheit

Mit dem Gebot der Angemessenheit sind automatisierte Kfz-Kennzeichenkontrollen nur vereinbar, wenn die Ermächtigungsgrundlage hinreichend begrenzt ist und übergreifende Anforderungen an Kontrolle und Datennutzung beachtet sind. Es bedarf stets eines die konkrete Kontrolle rechtfertigenden Grundes, der auf einer hinreichenden Tatsachenbasis beruht und dem staatlichen

---

[12] stRspr. des BVerfG, siehe BVerfGE 150, 244 (278 f.).

[13] Vgl. LT-Drs. 8/5018, S. 41

[14] BVerfGE 150, 244 (280).

[15] BVerfGE 150, 244 (280).

Handeln nachprüfbare Grenzen setzt.[16] Die automatisierte Erfassung von Kfz-Kennzeichen **darf nicht anlasslos erfolgen oder flächendeckend durchgeführt werden**,[17] was vornehmlich § 16b Abs. 2 SOG LSA sicherstellt.

aa) Kennzeichenerfassung gemäß § 16b Abs. 1 S. 1 Nr. 1 SOG LSA

§ 16b Abs. 1 S. 1 Nr. 1 SOG LSA erlaubt die **Schleierfahndung**, d.h. konkret an den in § 14 Abs. 3 S. 1 SOG LSA genannten Orten unter den Voraussetzungen des § 14 Abs. 3 S. 1 und 2 , § 20 Abs. 2 S. 1 Nrn. 1, 3 bis 6 SOG LSA die offene oder verdeckte[18] Erfassung von Kfz-Kennzeichen (sowie Ort, Datum, Uhrzeit und Fahrtrichtung) durch den Einsatz automatisierter Kennzeichenerkennungssysteme. Die Ermächtigungsgrundlage lässt sich verfassungsrechtlich durch das Ziel rechtfertigen, als **Ausgleich für den Wegfall von Grenzkontrollen** einer hierdurch erleichterten Begehung bestimmter Straftaten entgegenzutreten. Erforderlich ist dafür jedoch eine hieran orientierte konsequente und klare Begrenzung der Zwecke und Orte solcher Kontrollen. Verhältnismäßig sind automatisierte Kfz-Kennzeichenkontrollen danach nur in dem Umfang, in dem sie einen konsequenten Grenzbezug haben und dieser gesetzlich in einer den Bestimmtheitsanforderungen genügenden Weise gesichert ist.[19]

Der Gesetzgeber hat folglich sicherzustellen, dass nur **Orte mit einem klaren Grenzbezug** in Betracht kommen.[20] Unklare Regelungen, die dazu führen können, dass sich der Grenzbezug in der Praxis verliert und sich Kontrollen allgemein in das Landesinnere verschieben, sind damit

---

[16] BVerfGE 150, 244 (282)

[17] Vgl. BVerfGE 120, 378 (430).

[18] Verfassungsrechtlich unbedenklich ist es, dass die Kennzeichenkontrollen verdeckt durchgeführt werden können (wohl a.A.: Roßnagel, NJW 2008, 2547 (2550)). Dies ist zur Erreichung der erstrebten Zwecke geeignet und erforderlich und durch sie gerechtfertigt. Anders als für heimliche Überwachungsmaßnahmen von höherer Eingriffsintensität bedarf es insoweit keiner Benachrichtigungspflicht. Das gilt auch im Trefferfall. Vielmehr reicht es unter Verhältnismäßigkeitsgesichtspunkten, wenn die Betroffenen von den Kontrollen nur i.R.v. ihnen gegenüber ergriffenen Folgemaßnahmen erfahren und deren Rechtmäßigkeit dann fachgerichtlich überprüfen lassen können. Zu berücksichtigen ist ergänzend, dass – auch wenn für die Kennzeichenerfassung in der Praxis wohl nur ausnahmsweise zielführend – darüber hinaus auch der allgemeine datenschutzrechtliche Auskunftsanspruch besteht. Siehe BVerfGE 150, 244 (302).

[19] BVerfGE 150, 244 (299).

[20] BVerfGE 150, 244 (299).

unvereinbar. Während bloße Durchgangsstraßen nach der Rechtsprechung des BVerfG diesen Anforderungen nicht genügen, erfüllen Bundesfernstraßen sie.[21] Aus § 14 Abs. 3 S. 1 SOG LSA ergibt sich, dass die Kontrollen nur an Bundesfernstraßen, an Autohöfen sowie an der Straßenverbindung zwischen Autobahn und Autohof zulässig sein sollen. An diesen Orten lässt sich der erforderliche Grenzbezug bejahen. Auch wenn Autohöfe im Unterschied zu Autobahnraststätten von Bundesfernstraßen räumlich entfernt liegen, besteht jedoch ein enger Zusammenhang zwischen ihnen und dem dortigen bzw. internationalen Autoverkehr.

bb) Kennzeichenerfassung gemäß § 16b Abs. 1 S. 1 Nr. 2 SOG LSA

Dem erheblichen Eingriffsgewicht automatisierter Kfz-Kennzeichenkontrollen entspricht es, dass sie zu ihrer Rechtfertigung jeweils auf Gründe gestützt werden müssen, die dem Schutz von **Rechtsgütern von zumindest erheblichem Gewicht** oder sonst einem vergleichbar gewichtigen öffentlichen Interesse dienen.[22] Zu diesen Rechtsgütern zählen vornehmlich die besonders schutzwürdigen Rechtsgüter wie Leib, Leben und Freiheit der Person und der Bestand und die Sicherheit des Bundes und der Länder.[23] Vor diesem Hintergrund ist die Rechtsgrundlage des § 16b Abs. 1 S. 1 Nr. 2 SOG LSA **verfassungskonform**. Denn sie setzt die Abwehr einer erheblichen Gefahr voraus. Eine erhebliche Gefahr ist eine Gefahr für ein bedeutsames Rechtsgut, wie Leben, Gesundheit, Freiheit, wesentliche Vermögenswerte oder den Bestand des Staates (§ 3 Nr. 3 lit. c SOG LSA).

cc) Datenabgleich gemäß § 16b Abs. 1 S. 2 und S. 3 SOG LSA

§ 16b Abs. 1 S. 2 und S. 3 SOG LSA enthalten eine Ermächtigungsgrundlage für den Abgleich der KfZ-Kennzeichen mit polizeilichen Fahndungsbeständen. Die Reichweite dieser Regelungen ergibt sich zwar nicht eindeutig aus dem Gesetzentwurf selbst, sie lässt sich aber **verfassungskonform eng**

[21] BVerfGE 150, 244 (300); 150, 309 (337).

[22] BVerfGE 150, 244 (284); 150, 309 (336); Braun, in: Heusch/Ullrich/Posser (Hrsg.), VerfassungsR-HdB, 2024, § 7 Rn. 131.

[23] BVerfGE 120, 274 (328); 150, 244 (284).

auslegen und ist daher nicht verfassungswidrig.[24] Nach der bundesverfassungsgerichtlichen Rechtsprechung erlauben § 16b Abs. 1 S. 2 und S. 3 SOG LSA nicht pauschal, einen Abgleich mit allen dort genannten Fahndungsbeständen vorzunehmen. Vielmehr muss die Polizei stets eine auf den jeweiligen Zweck der Kennzeichenerfassung bezogene **Auswahl der Fahndungsbestände** vornehmen.[25] § 16b Abs. 1 S. 2 und S. 3 SOG LSA genügen auch den verfassungsrechtlichen **Bestimmtheitsanforderungen**. Es ist insbesondere nicht zu beanstanden, dass sie die zum Abgleich eröffneten Fahndungsbestände nur abstrakt, nicht aber unter Verweis auf konkrete Dateien umschreiben.[26]

dd) Löschpflichten gemäß § 16b Abs. 3 S. 1 SOG LSA

Es bestehen keine verfassungsrechtlichen Bedenken im Hinblick auf die Gewährleistung von Löschungsregelungen. § 16b Abs. 3 S. 1 SOG LSA sieht eine strikt an den Zwecken orientierte Regelung zur Löschung der erhobenen Daten vor.[27]

ee) Fehlende Dokumentationspflicht

Die Ermächtigung zur Kennzeichenerfassung kann indes nur dann als verhältnismäßig angesehen werden, wenn die **Entscheidungsgrundlagen für die Durchführung einer solchen Maßnahme nachvollziehbar und überprüfbar dokumentiert** werden.[28] Denn die Entscheidung über die Einrichtung einer Kennzeichenkontrolle wird – anders als zu begründende Verwaltungsakte – den Betroffenen in keiner Weise mitgeteilt. Als verdeckte Maßnahmen werden die Kontrollen überhaupt nur in den Trefferfällen bekannt und auch dann grundsätzlich nicht begründet. Für die Verhältnismäßigkeit ist dies – bezogen auf alle Fälle der Kfz-Kennzeichenkontrolle – von dreifacher

[24] Vgl. BVerfGE 150, 244 (287); 150, 309 (340 f.).

[25] BVerfGE 150, 244 (287); Braun, in: Heusch/Ullrich/Posser (Hrsg.), VerfassungsR-HdB, 2024, § 7 Rn. 131.

[26] BVerfGE 150, 244 (288).

[27] Vgl. BVerfGE 150, 244 (304).

[28] BVerfGE 150, 244 (303); vgl. BVerfGE 133, 277 (370); 150, 309 (342); SächsVerfGH, Urt. v. 10.7.2003, Az.: Vf. 43-II-00, juris, Rn. 218 ff. = BeckRS 2003, 12595.

Bedeutung:[29] 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 den **Datenschutzbeauftragten**, der in Fällen eingeschränkter individualrechtlicher Rechtsschutzmöglichkeiten wie hier gesteigerte Bedeutung zukommt. Schließlich wird damit die **verwaltungsgerichtliche Kontrolle** erleichtert, wenn solche Maßnahmen bekannt werden.

Mit den Anforderungen des Verhältnismäßigkeitsgrundsatzes ist es daher nicht vereinbar, dass § 16b SOG LSA **keine ausreichende Dokumentationspflicht** der Entscheidungsgrundlagen für den Einsatz automatisierter Kennzeichenkontrollen vorsieht.[30] Zwar hält § 16b Abs. 2 S. 2 SOG LSA fest, dass Ort, Zeit und Umfang der Maßnahmen nach § 16b Abs. 1 SOG LSA sowie die Auswahl der Fahndungsbestände oder Dateisysteme vom Behördenleiter oder von einer von ihm beauftragten Person angeordnet werden müssen. Aber aus diesem „**Behördenleitervorbehalt**“ geht insbesondere nicht hervor, dass die Anordnung schriftlich erfolgen muss (im Unterschied zu anderen Vorschriften des SOG LSA, die ausdrücklich festhalten: „Die Anordnung ergeht schriftlich“). **Ohne Verschriftlichung kann eine Anordnung keine Dokumentationswirkung entfalten**. Außerdem verpflichtet § 16b Abs. 2 S. 2 SOG LSA – bspw. im Unterschied zum reformierten Art. 39 Abs. 2 S. 2 BayPAG – nicht ausdrücklich dazu, die wesentlichen Gründe für die Maßnahmenanordnung anzugeben.

d) Fazit

Die Ermächtigungsgrundlagen des § 16b Abs. 1 SOG LSA sind grundsätzlich verfassungsgemäß. Die vorgeschlagene Befugnisnorm ist gleichwohl mit dem Grundrecht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG unvereinbar, soweit sie keine ausreichende Dokumentationspflicht vorsieht. **Der Landtag sollte die Vorschrift daher dringend nachbessern.**

---

[29] BVerfGE 150, 244 (303).

[30] Vgl. BVerfGE 150, 244 (302 f.).

C. Automatisierte Datenanalyse (§ 30a SOG LSA)

Mit dem vorgeschlagenen § 30a SOG LSA soll die Polizei erstmalig eine Ermächtigungsgrundlage für operative und strategische Datenanalysen erhalten. Auch wenn derartige Instrumente entscheidend dafür sind, die Gefahrenabwehr fortzuentwickeln und an eine immer stärker datafizierte Welt anzupassen, wirft ihre Einführung ernstzunehmende Rechtsfragen auf.

I. Verfassungskonformität

Die Verfassungskonformität des § 30a SOG LSA bestimmt sich in erster Linie danach, inwieweit die Vorschrift die **bundesverfassungsgerichtlichen Maßstäbe zum polizeilichen Data-Mining** einhält. Konkret hat das BVerfG im Jahr 2023 die Ermächtigungsgrundlagen des § 25a HSOG (Automatisierte Anwendung zur Datenanalyse)[31] und des § 49 HmbPolDVG (Automatisierte Anwendung zur Auswertung vorhandener Daten) geprüft und in Teilen für verfassungswidrig befunden.[32]

1. Grundrechtseingriff

Werden gespeicherte Datenbestände mittels einer automatisierten Anwendung zur Datenanalyse verarbeitet, greift dies in das Grundrecht auf **informationelle Selbstbestimmung** (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) aller ein, deren Daten bei diesem Vorgang personenbezogen Verwendung finden.[33] Mit der automatisierten Auswertung gespeicherter Daten erlaubt § 30a SOG LSA eine weitere Nutzung früher erhobener Daten über den ursprünglichen Anlass hinaus. Das begründet einen neuen Grundrechtseingriff und muss verfassungsrechtlich eigens nach dem **Grundsatz der Zweckbindung** gerechtfertigt werden.[34] Indessen liegt ein Grundrechtseingriff hier nicht nur in der

---

[31] Weiterführend z.B. Santhakumar, „Legal Design“ für HessenData (§ 25a HSOG) – ein abgestuftes Kontrollkonzept, in: Botta et al. (Hrsg.), Rechtsfragen virtueller Welten, 2025, S. 103 (105 ff.).

[32] BVerfGE 165, 363 (363 ff.).

[33] BVerfGE 165, 363 (388).

[34] BVerfGE 165, 363 (388); vgl. BVerfGE 141, 220 (324 und 327).

weiteren, zusammenführenden Verwendung vormals getrennter Daten, sondern darüber hinaus in der Erlangung besonders grundrechtsrelevanten **neuen Wissens**, das durch die automatisierte Datenanalyse geschaffen werden kann.[35]

2. Rechtfertigung

Der Grundrechtseingriff durch die automatisierte Datenanalyse lässt sich jedoch grundsätzlich rechtfertigen.[36] Dies hängt insbesondere von der **materiellen Verfassungsmäßigkeit** des § 30a SOG LSA, d.h. von seiner Verhältnismäßigkeit, ab (vgl. oben B. II. 2.).

a) Legitimer Zweck

§ 30a SOG LSA dient dem legitimen Zweck der **polizeilichen Aufgabenerfüllung**.[37]

b) Geeignetheit und Erforderlichkeit

§ 30a SOG LSA ist zu diesem Zweck förderlich, d.h. geeignet. Mangels gleich geeigneter, milderer Mittel ist § 30a SOG LSA auch erforderlich. Insbesondere zeichnen sich automatisierte Datenanalysen im **Unterschied zu manuellen Datenabgleichen** dadurch aus, dass sie darauf gerichtet sind, neues Wissen zu erzeugen.[38] Unter Zeitdruck lassen sich die stetig wachsenden Datenmengen zudem überhaupt nur noch schwer manuell auswerten.[39]

c) Angemessenheit

Spezielle Anforderungen für die automatisierte Datenanalyse durch Polizeibehörden ergeben sich aus dem Gebot der Angemessenheit. Wie streng diese Anforderungen im Einzelnen sind, bestimmt sich

---

[35] BVerfGE 165, 363 (388 f.); Graulich, NVwZ-Beilage 2023, 27 (30); vgl. BVerfGE 156, 11 (39 f.).

[36] BVerfGE 165, 363 (388);

[37] LT-Drs. 8/5018, S. 56 f.

[38] LT-Drs. 8/5018, S. 57.

[39] Vgl. BVerfGE 165, 363 (389).

nach dem **Eingriffsgewicht der Maßnahme**.[40] Das Eingriffsgewicht einer automatisierten Datenanalyse und die Anforderungen an deren verfassungsrechtliche Rechtfertigung hängen zum einen vom **Gewicht der vorausgegangenen Datenerhebungseingriffe** ab.[41] Dann sind die Grundsätze der Zweckbindung und Zweckänderung maßgeblich. Zum anderen hat die automatisierte Datenanalyse ein **Eigengewicht**, da die Weiterverarbeitung spezifische Belastungen mit sich bringen kann, die über das Eingriffsgewicht der ursprünglichen Datenerhebung hinausgehen.[42] In diesem Zusammenhang ergeben sich aus dem Gebot der Angemessenheit zusätzliche Rechtfertigungsanforderungen.

aa) Eingriffsintensität der Datenanalyse

Diese weitergehenden Rechtfertigungsanforderungen an eine automatisierte Datenanalyse variieren nach deren Eingriffsintensität.[43] Der Gesetzgeber kann den Umfang der Rechtfertigungsanforderungen daher bewusst steuern, indem er die maßgeblichen Faktoren für die Eingriffsintensität regelt.

Entscheidend für die Eingriffsintensität ist insbesondere, wie viele Grundrechtsträger wie intensiven Beeinträchtigungen ausgesetzt sind und unter welchen Voraussetzungen dies geschieht, insbesondere ob diese Personen hierfür einen Anlass gegeben haben.[44] Die Landesregierung hat sich erkennbar darum bemüht, auf diesem Wege die Eingriffsintensität des § 30a SOG LSA zu reduzieren. So nennt § 30a Abs. 4 S. 1 SOG LSA **Kategorien betroffener Personen**, deren Daten nach § 30a Abs. 4 S. 2 SOG LSA auf einer Analyseplattform automatisiert zusammengeführt werden dürfen, was einer Eingrenzung der Betroffenheit dienlich ist. Gleichwohl ist von einer erheblichen Anzahl potenziell Betroffener auszugehen. So erfasst bspw. § 30a Abs. 4 S. 1 Nr. 7 SOG LSA u.a. Auskunftspersonen,

---

[40] stRspr. des BVerfG, siehe BVerfGE 165, 363 (389); Graulich, NVwZ-Beilage 2023, 27 (31); vgl. BVerfGE 141, 220 (269).

[41] BVerfGE 165, 363 (390).

[42] BVerfGE 165, 363 (390); Bäuerle, ZD 2025, 128 (130).

[43] BVerfGE 165, 363 (398).

[44] BVerfGE 165, 363 (399).

Hinweisgeber, Kontaktpersonen, Opfer und Zeugen einer zukünftigen Straftat und § 30a Abs. 4 S. 1 Nr. 9 SOG LSA alle Personen, deren personenbezogene Daten im Zusammenhang mit der Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten durch die Polizei verarbeitet werden (also ebenfalls nicht nur Beschuldigten-, sondern u.a. auch Opfer- und Zeugendaten**)**. Dies erhöht die **„Streubreite" der Grundrechtseingriffe** deutlich. Eingriffsverschärfend wirkt sich zudem aus, dass § 30a SOG LSA keine besonderen Schutzmaßnahmen im Fall der Erstellung von **individuellen Bewegungs- oder Verhaltensprofilen** aufstellt.[45] Wie sich aus § 30a Abs. 3 SOG LSA ergibt, soll derartiges Profiling von der Ermächtigungsgrundlage umfasst sein (zur Unionskonformität siehe unten C. II.).

(1) Art und Umfang der verarbeitbaren Daten

Das Eingriffsgewicht wird darüber hinaus insbesondere durch **Art und Umfang der verarbeitbaren Daten** bestimmt.[46] Je größer die **Menge an personenbezogenen Daten** ist, die in die automatisierte Datenanalyse einbezogen werden kann – und je weniger der Gesetzgeber die verwendbare Datenmenge begrenzt –, desto schwerer wiegt der Eingriff.[47] Dabei ist die Regelung der Menge der verwendbaren Daten eng mit der Festlegung der Art der Daten verknüpft. Je weniger die Art der verwendbaren Daten eingeschränkt wird, desto größer fällt die verarbeitbare Datenmenge aus, was tendenziell das Eingriffsgewicht erhöht.[48]

(a) Herkunft der Daten

Das Eingriffsgewicht kann durch gesetzliche Regelungen zur Herkunft der Daten verringert werden: bspw. durch eine Beschränkung auf Daten, die von der Behörde selbst oder von einer anderen Behörde desselben Landes – zumindest jedoch einer anderen **inländischen Behörde** – erhoben

[45] Vgl. BVerfGE 165, 363 (400).

[46] BVerfGE 165, 363 (401 ff.).

[47] BVerfGE 165, 363 (401).

[48] BVerfGE 165, 363 (401).

wurden.[49] Auch der Ausschluss von Daten aus **sozialen Netzwerken** oder der Ausschluss von Daten, die von **nachrichtendienstlichen Behörden** stammen, kann die Eingriffsintensität abmildern.[50]

Gemessen an diesen Vorgaben bewirkt § 30a Abs. 4 S. 2 SOG LSA zwar eine gewisse Reduzierung des Eingriffsgewichts, aber nicht in einem Ausmaß, das die gebotenen Rechtfertigungsanforderungen absenken würde. Konkret können Vorgangsdaten, Falldaten, Daten aus dem Informationssystem der Polizei, zum Abruf durch die Polizei im polizeilichen Informationssystem zwischen Bund und den Ländern bereitstehende Daten (INPOL-neu), Daten aus dem polizeilichen Informationsaustausch, Verkehrsdaten aus Funkzellenabfragen, Telekommunikationsdaten und Daten aus Asservaten zusammengeführt werden (§ 30a Abs. 4 S. 2 SOG LSA). Eine herkunftsbezogene Beschränkung auf Daten, die ursprünglich **durch inländische Polizeibehörden** erhoben worden sind, findet sich in der Regelung **nicht** niedergelegt. So dürfte es bspw. zulässig sein, personenbezogene Daten, die **Nachrichtendienste** an Polizeibehörden übermittelt haben (z.B. nach § 19 BVerfSchG, § 11 BNDG oder § 11 MADG) und sich somit nunmehr in den polizeilichen Datenbeständen befinden, in eine Analyseplattform einzuspeisen.

Insbesondere die Einbeziehung von **Vorgangsdaten** trägt erheblich zum Volumen der Datenanalyse bei.[51] Ein „Vorgang“ umfasst sämtliche Unterlagen, die im Zusammenhang einer polizeilichen Tätigkeit über eine bestimmte Person, Sache oder einen sonstigen Gegenstand polizeilichen Handelns geführt werden.[52] In den Vorgangsbearbeitungssystemen erfasst die Polizei Daten, die sie für ihre konkrete polizeiliche Aufgabe und Sachbearbeitung im Einzelfall benötigt. Aufgenommen werden insbesondere Anzeigen, Ermittlungsberichte und Vermerke (auch zu Verkehrsunfällen). Die Systeme enthalten auch Daten zu Personen, die Anzeige erstatten oder Hinweise geben, zu Zeugen,

[49] BVerfGE 165, 363 (401).

[50] BVerfGE 165, 363 (401).

[51] Vgl. BVerfGE 165, 363 (422).

[52] Müller/Schwabenbauer, in: Lisken/Denninger (Hrsg.), Handbuch des Polizeirechts, 7. Aufl. 2021, Abschnitt G, Rn. 832 m.w.N.

Unfallbeteiligten und anderen Personen, die nicht Verdächtige oder Beschuldigte i.S.d. Strafprozessrechts oder Verantwortliche i.S.d. Polizeirechts sind.

Positiv zu vermerken ist zwar, dass eine direkte Anbindung der Analyseplattform an der **Allgemeinheit offenstehende Netzwerke** unzulässig ist (§ 30a Abs. 4 S. 4 SOG LSA). Eine Relativierung erfährt dieses Verbot aber durch § 30a Abs. 4 S. 3 SOG LSA, wonach die Polizei u.a. einzelne gesondert gespeicherte Daten aus allgemein zugänglichen Quellen (z.B. Social Media oder Online-Foren) ergänzend auf der Analyseplattform zusammenführen kann.[53] Dieselbe Regelung erlaubt der Polizei zudem auch, personenbezogene Daten aus gezielten Abfragen in gesondert geführten staatlichen Registern (z.B. Melde- oder Waffenregister) in der Analyseplattform zusammenzuführen.

Eingriffsmildernd wirkt der Ausschluss der Verarbeitung von Daten, die ursprünglich durch **besonders schwere Grundrechtseingriffe** erlangt wurden. Insofern ist es zu begrüßen, dass auf einer Analyseplattform gemäß § 30a Abs. 4 S. 5 SOG LSA keine personenbezogenen Daten zusammengeführt werden dürfen, die durch Wohnraumüberwachung oder Online-Durchsuchung nach der StPO oder Maßnahmen nach § 17 Abs. 4 oder § 17b Abs. 1 SOG LSA erlangt wurden. Gleichwohl mangelt es an einer weitergehenden Regelung, die auch Beschränkungen für die Verarbeitung von Informationen vorsieht, die aus anderen besonders eingriffsintensiven Maßnahmen resultieren, wie bspw. aus einer Telekommunikationsüberwachung, einer langfristigen Observation oder dem Einsatz Verdeckter Ermittler.[54] Da § 30a Abs. 4 S. 2 SOG LSA ausdrücklich die Verarbeitung von Telekommunikationsdaten einschließt, ist neben der informationellen Selbstbestimmung auch das **Fernmeldegeheimnis des Art. 10 Abs. 1 Var. 3 GG** („Telekommunikationsgeheimnis“) berührt.

[53] Vgl. Zöller, Schriftliche Stellungnahme zum Gesetzentwurf der Landesregierung für ein Landesgesetz zur Änderung des Polizei- und Ordnungsbehördengesetzes vom 6. November 2024 (RLP-LT-Drs. 18/10756), S. 18.

[54] Vgl. Zöller, Schriftliche Stellungnahme zum Gesetzentwurf der Landesregierung für ein Landesgesetz zur Änderung des Polizei- und Ordnungsbehördengesetzes vom 6. November 2024 (RLP-LT-Drs. 18/10756), S. 17.

(b) Datenarten und -formate

Eine Chance zur Eingriffsmilderung hat die Landesregierung verpasst, indem sie eine **Regelung zugelassener Datenarten** (vgl. etwa § 3 Abs. 1 ATDG oder § 29 Abs. 2a S. 3 GwG) unterlassen hat.[55] Auch eine Regelung der **einbeziehbaren Dateiformate** (Bilder, Video- und Audioaufnahmen) oder ein **Ausschluss biometrischer Daten** finden sich in § 30a SOG LSA nicht. Eine damit einhergehende Eingriffsmilderung kann erst aus der Rechtsverordnung nach § 30a Abs. 8 SOG LSA erfolgen. Getreu der **Wesentlichkeitstheorie** sollte es der parlamentarische Gesetzgeber sein, der klare Leitplanken für die Datenauswahl aufstellt.

(c) Zugriffsbeschränkung

Auch eine technisch und organisatorisch gesicherte **Zugriffsbeschränkung auf eine begrenzte Mitarbeiteranzahl und eine besondere Qualifizierung dieser Personen** kann praktisch die Menge der durch Datenanalyse verarbeitbaren personenbezogenen Daten begrenzen: Je weniger Personen Zugriff auf das Analyseinstrument haben und je gezielter dieser Zugriff erfolgt, desto weniger Analysevorgänge werden voraussichtlich ausgelöst und desto weniger Daten werden verarbeitet.[56] Auch dieses Instrument zur Eingriffsmilderung hat die Landesregierung – abgesehen von der Regelung in § 30a Abs. 3 S. 3 SOG LSA („Eine operative oder strategische Datenanalyse wird durch zugriffsberechtigte Polizeibeamte manuell ausgelöst […]“) – der Verordnung nach § 30a Abs. 8 SOG LSA überlassen. Dass die Grundrechtssensibilität der Analyseplattformen in der Praxis nicht zwangsläufig mit einem begrenzten Kreis von Berechtigten einhergeht, zeigt beispielhaft der Fall Hessen, wo zeitweise Hunderte von Beschäftigten Zugriff auf die Analyseanwendung (HessenData) hatten.[57]

---

[55] Vgl. BVerfGE 165, 363 (404).

[56] BVerfGE 165, 363 (404).

[57] Zöller, Schriftliche Stellungnahme zum Gesetzentwurf der Landesregierung für ein Landesgesetz zur Änderung des Polizei- und Ordnungsbehördengesetzes vom 6. November 2024 (RLP-LT-Drs. 18/10756), S. 17 f.

(d) Entstehung einer „Super-Datenbank“?

Als das BVerfG über die Verfassungsmäßigkeit der Ermächtigungsgrundlagen aus Hamburg und Hessen entschieden hat, hatte es erkennbar keine **dauerhafte Zusammenführung der polizeilichen Datenbestände**, sondern vielmehr eine anlassbezogene Zusammenführung zwecks automatisierter Datenanalyse vor Augen.[58] Auch der Wortlaut des § 30a Abs. 4 S. 1 SOG LSA spricht für ein solches Verständnis. Gleichwohl ist die Entstehung einer „Super-Datenbank“ keineswegs ausgeschlossen, sondern vielmehr das ausdrückliche Ziel der Vorschrift, wie sich aus ihrer Begründung ergibt. Darin heißt es u.a., dass „ein aufbereiteter Datenbestand für operative Analysen unmittelbar zur Verfügung stehen muss“.[59] Sollte mit § 30a SOG LSA tatsächlich der Aufbau einer „Super-Datenbank“ einhergehen, wäre der daraus folgende Grundrechtseingriff nicht nur von eigenem Gewicht,[60] sondern derart gewichtig, dass die Norm schon aus diesem Grund **verfassungswidrig** wäre.[61] Denn im Unterschied zur konkreten Datenanalyse stellt § 30a SOG LSA für die Datenzusammenführung jenseits der anlassbezogenen Analyse **keine Rechtmäßigkeitsvoraussetzungen** auf, die den Maßstäben des BVerfG entsprechen würden (insbesondere das Erfordernis einer zumindest hinreichend konkretisierten Gefahr für besonders gewichtige Rechtsgüter; vgl. unten C. I. 2. c) bb)). **Der Landtag sollte daher dringend klarstellen, dass eine solche umfassende und anlasslose Datenzusammenführung nicht beabsichtigt ist.**

(2) Zugelassene Methode der Datenanalyse

Zusätzlich beeinflusst die zugelassene Methode der Datenanalyse die Eingriffsintensität.

---

[58] Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Stellungnahme zum Entwurf eines Gesetzes zur Verbesserung der Terrorismusbekämpfung, BT-Drs. 20/12806, Ausschuss-Drs. 20(4)483, S. 8.

[59] LT-Drs. 8/5018, S. 58.

[60] Vgl. zum Eingriffsgewicht einer heimlichen, vorsorgenden Datenspeicherung BVerfG, NVwZ 2024, 1736 (1748 ff.).

[61] Vgl. Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, Stellungnahme zum Entwurf eines Gesetzes zur Verbesserung der Terrorismusbekämpfung, BT-Drs. 20/12806, Ausschuss-Drs. 20(4)483, S. 8; Kipker, Schriftliche Stellungnahme zum Entwurf eines Gesetzes zur Verbesserung der Terrorismusbekämpfung, BT-Drs. 20/12806, Ausschuss-Drs. 20(4)493 J, S. 15 f.

(a) Komplexität des Datenabgleichs

Besonders hohe Eingriffsintensität kann der Einsatz komplexer Methoden des Datenabgleichs haben.[62] Wenn die Polizei mithilfe aller verfügbaren informationstechnischen Möglichkeiten aus den vorhandenen Daten weitreichende Erkenntnisse gewinnt, neue Zusammenhänge erschließt, durch mehrstufige Analysen neue Verdachtsmomente erzeugt und daraufhin weitere Analyseschritte oder operative Maßnahmen einleitet, können die negativen Auswirkungen einer automatisierten Datenanalyse für die Betroffenen erheblich sein.[63] Das Gewicht der individuellen Beeinträchtigung wird dadurch deutlich erhöht. Bei komplexen Datenabgleichen kommt hinzu, dass die Möglichkeit, Fehler zu erkennen und zu korrigieren, erschwert wird – vor allem aufgrund der **mangelnden Nachvollziehbarkeit der eingesetzten Algorithmen**.[64] Dies erschwert Rechtsschutz und externe Kontrolle erheblich. Insgesamt ist die Methode der automatisierten Datenanalyse umso eingriffsintensiver, je mehr und tiefere Erkenntnisse über Personen erlangt werden können, je höher die Anfälligkeit für Fehler und Diskriminierung ist und je schwerer die softwaregestützten Verknüpfungen nachvollzogen werden können.[65]

Im Gesetzentwurf findet sich zwar eine abschließende Beschreibung der zugelassenen Verarbeitungsmethoden. Diese ist aber sehr weitreichend. Gemäß § 30a Abs. 5 S. 1 SOG LSA sind die zulässigen Methoden und Techniken der automatisierten Datenanalyse die deskriptive Analytik, diagnostische Analytik, prädiktive Analytik, präskriptive Analytik, Data-Mining, maschinelles Lernen, Data Science und Sekundärdatenanalyse. Zudem hält die Gesetzesbegründung ausdrücklich fest, dass die Norm technikneutral ist.[66] Vor diesem Hintergrund erlaubt § 30a SOG LSA insbesondere auch den **Einsatz von KI-Systemen**. Dem steht nicht entgegen, dass die Vorschrift

[62] BVerfGE 165, 363 (404).

[63] BVerfGE 165, 363 (404 f.).

[64] BVerfGE 165, 363 (405); vgl. BVerfGE 154, 152 (259 f.).

[65] BVerfGE 165, 363 (405).

[66] LT-Drs. 8/5018, S. 57.

gemäß der Gesetzesbegründung **keine Befugnis zum Anlernen derartiger Systeme** beinhaltet.[67] Fraglich ist schon, inwieweit diese Aussage mit dem zulässigen Einsatz maschinellen Lernens vereinbar ist. Jedenfalls können KI-Systeme rechtskonform zum Einsatz kommen, die bereits auf der Grundlage anderer Datenbestände (z.B. ausländischer Polizeibehörden) trainiert worden sind.[68] So können besonders tiefgehende Informationen und Annahmen über eine Person erzeugt werden, deren Korrektheit sich unter Umständen nur erschwert überprüfen lässt. Komplexe algorithmische Systeme können sich im Verlauf des maschinellen Lernprozesses – auch wenn dieser bereits vor dem polizeilichen Einsatz in Sachsen-Anhalt abgeschlossen wurde – zunehmend von der ursprünglichen menschlichen Programmierung entfernen.[69] Dies würde dazu führen, dass die maschinellen Lernprozesse und die Ergebnisse der Anwendung **immer schwerer nachvollziehbar** werden. In einem solchen Fall droht die staatliche Kontrolle über diese Anwendung verloren zu gehen. Wird Software von **privaten Akteuren oder ausländischen Staaten** eingesetzt, steigt zudem das Risiko unbemerkter Manipulation oder des unerkannten Zugriffs auf Daten durch Dritte (siehe unten C. III.).[70] Eine zusätzliche Herausforderung besteht darin, die Entstehung und Nutzung **diskriminierender Algorithmen** zu verhindern. Die Regelung des § 30a Abs. 5 S. 2 SOG LSA dürfte dafür nicht ausreichen.

(b) Offenheit des Suchvorgangs

Das Eingriffsgewicht ist außerdem umso größer, je offener die Methode des Suchvorgangs ist und je weniger die automatisierte Datenanalyse durch **polizeiliche Suchmuster** gesteuert wird, die auf spezifischen Erkenntnissen und Annahmen zum konkreten Sachverhalt beruhen.[71] Das Eingriffsgewicht steigt insbesondere, wenn die Datenanalyse nicht auf einem **Suchbegriff** basiert, der sich auf den bislang erkennbaren Sachverhalt bezieht – wie es bspw. in § 65a Abs. 2 S. 2 POG

[67] LT-Drs. 8/5018, S. 57.

[68] Vgl. LT-Drs. 8/5018, S. 16.

[69] BVerfGE 165, 363 (408).

[70] BVerfGE 165, 363 (408).

[71] BVerfGE 165, 363 (405 f.).

RLP vorgesehen ist: „Die automatisierte Datenanalyse wird manuell ausgelöst und erfolgt anhand von Suchbegriffen, die sich aus einem konkreten Sachverhalt, bezogen auf einen Anlass im Sinne des Absatzes 1 ergeben; bei Maßnahmen nach Absatz 1 Nr. 2 und 3 ist der Suchvorgang zudem auf die nach den §§ 4 und 5 Verantwortlichen auszurichten." Wenn die Analyse jedoch darauf abzielt, lediglich statistische Auffälligkeiten in den Datenmengen zu entdecken, die anschließend in weiteren automatisierten Abgleichschritten mit bestimmten Datenbeständen verknüpft werden, können daraus neue Informationen entstehen, nach denen die Polizei zuvor keinen Anlass zur Suche hatte.[72] Diesbezüglich finden sich in § 30a SOG LSA keine konkreten Vorgaben.

(c) Art der Suchergebnisse

Das Eingriffsgewicht hängt darüber hinaus davon ab, welche Art von Suchergebnissen durch eine automatisierte Datenanalyse erzielt wird.[73] Besonders eingriffsintensiv erweist es sich, wenn die automatisierte Anwendung **personenbezogene Erkenntnisse** liefert und dabei maschinelle Sachverhaltsbewertungen enthält, die über die bloße Anzeige von Übereinstimmungen zwischen dem Suchkriterium und den durchsuchten Daten hinausgehen.[74] Das gilt vor allem, wenn i.R.v. **Predictive Policing** maschinell Gefährlichkeitsaussagen über Personen getroffen werden (vgl. unten C. II.). Diesbezüglich finden sich in § 30a SOG LSA ebenfalls keine konkreten Schutzmaßnahmen.

(3) Zwischenfazit

Im Ergebnis ergeben sich aus § 30a SOG LSA – trotz der begrüßenswerten Anstrengungen der Landesregierung, die Eingriffsintensität abzumildern – schwerwiegende Eingriffe in die informationelle Selbstbestimmung. **Eine besondere Eingriffsintensität ginge von der Schaffung einer „Super-Datenbank" aus, die schon für sich die Verfassungswidrigkeit der Regelung zur Folge hätte.**

---

[72] BVerfGE 165, 363 (406).

[73] BVerfGE 165, 363 (407).

[74] BVerfGE 165, 363 (407).

bb) Rechtfertigungsanforderungen

Ermöglicht die automatisierte Datenanalyse einen **schwerwiegenden Eingriff** in die informationelle Selbstbestimmung, ist dies nach der Rechtsprechung des BVerfG grundsätzlich nur unter den engen Voraussetzungen zu rechtfertigen, wie sie allgemein für eingriffsintensive heimliche Überwachungsmaßnahmen gelten, also nur zum **Schutz besonders gewichtiger Rechtsgüter**, sofern für diese eine **zumindest hinreichend konkretisierte Gefahr** besteht.[75]

(1) Datenanalyse gemäß § 30a Abs. 6 S. 1 Nr. 1 SOG LSA

Der Tatbestand des § 30a Abs. 6 S. 1 Nr. 1 SOG LSA (**Abwehr einer erheblichen Gefahr**) erfüllt diese Anforderungen. Denn eine erhebliche Gefahr ist eine Gefahr für ein bedeutsames Rechtsgut, wie Leben, Gesundheit, Freiheit, wesentliche Vermögenswerte oder der Bestand des Staates (§ 3 Nr. 3 lit. c SOG LSA). Die Ermächtigungsgrundlage ist somit **verfassungskonform**.[76]

(2) Datenanalyse gemäß § 30a Abs. 6 S. 1 Nr. 2 SOG LSA

Anders ist der Tatbestand des § 30a Abs. 6 S. 1 Nr. 2 SOG LSA zu bewerten. Zwar greift die Vorschrift ersichtlich die Rechtsprechung des BVerfG zur zumindest **hinreichend konkretisierten Gefahr** auf, indem tatsächliche Anhaltspunkte die Annahme rechtfertigen müssen, dass innerhalb eines übersehbaren Zeitraumes auf eine zumindest ihrer Art nach konkretisierte Weise **Straftaten mit erheblicher Bedeutung** begangen werden und dies zur Verhinderung dieser Straftaten erforderlich ist. Aber der Regelungsvorschlag verankert damit **lediglich eine Bedingung** der konkretisierten Gefahr im Normtext. Denn zusätzlich müssen die Tatsachen den Schluss darauf zulassen, dass **bestimmte Personen** beteiligt sein werden, über deren Identität zumindest so viel bekannt ist, dass die staatliche Maßnahme gezielt gegen sie eingesetzt und weitgehend auf sie

[75] BVerfGE 165, 363 (410). Das Erfordernis einer zumindest hinreichend konkretisierten Gefahr für besonders gewichtige Rechtsgüter ist nur dann verfassungsrechtlich verzichtbar, wenn die zugelassenen Analyse- und Auswertungsmöglichkeiten durch Regelungen insbesondere zur Begrenzung von Art und Umfang der Daten und zur Beschränkung der Datenverarbeitungsmethoden normenklar und hinreichend bestimmt in der Sache so eng begrenzt sind, dass das Eingriffsgewicht der Maßnahmen erheblich gemindert ist.

[76] Vgl. Bäuerle, in: BeckOK PolR Hessen, 33. Ed. 1.6.2024, HSOG § 25a Rn. 32.

beschränkt werden kann.[77] Außerdem dient die Regelung nicht allein dem Schutz besonders gewichtiger Rechtsgüter. Straftaten mit erheblicher Bedeutung sind nach § 3 Nr. 4 SOG LSA stattdessen u.a. auch **gewerbs- oder bandenmäßig begangene Vergehen**, die sich in erster Linie gegen das Vermögen der Geschädigten richten (z.B. besonders schwerer Fall des Diebstahls nach § 243 StGB; Diebstahl mit Waffen, Bandendiebstahl, Wohnungseinbruchsdiebstahl nach § 244 StGB; Erpressung nach § 253 StGB etc.). Damit öffnet § 30a Abs. 6 S. 1 Nr. 2 den Rechtsgüterschutz deutlich „nach unten".[78] Die Voraussetzungen der Datenanalyse sind zudem auch zu **unbestimmt**, da § 3 Nr. 4 SOG LSA nicht abschließend ist („insbesondere") und es den Rechtsunterworfenen somit an hinreichender Klarheit darüber fehlt, wann sie im Fokus einer Analyse stehen können. Die Ermächtigungsgrundlage ist folglich **verfassungswidrig**.[79] Der Gesetzgeber sollte den Anwendungsbereich des § 30a Abs. 6 S. 1 Nr. 2 SOG LSA mithin dringend konkretisieren und einen abschließenden Katalog von Straftatbeständen aufnehmen.

(3) Datenanalyse gemäß § 30a Abs. 6 S. 1 Nr. 3 SOG LSA

Beim Tatbestand des § 30a Abs. 6 S. 1 Nr. 3 SOG LSA sieht der Gesetzentwurf noch nicht einmal eine zumindest hinreichend konkretisierte Gefahr vor („wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass Straftaten nach § 100a Abs. 2 oder § 100b Abs. 2 der Strafprozessordnung begangen werden sollen"). Allein der Umstand, dass bei einer derartigen Maßnahme zur vorbeugenden Straftatenbekämpfung keine Verkehrsdaten aus Funkzellenabfragen in die operative Datenanalyse einbezogen werden dürfen (§ 30a Abs. 6 S. 2 SOG LSA), macht dieses Erfordernis nicht entbehrlich.

§ 30a Abs. 6 S. 1 Nr. 3 SOG LSA regelt auch deshalb keine hinreichende Eingriffsschwelle, da über die zitierten StPO-Kataloge **auch Vorfeldtatbestände erfasst** sind (§§ 89a, 129, 129a, 129b, 149 StGB).[80] Zwar ist es dem Gesetzgeber verfassungsrechtlich nicht verwehrt, zur Bestimmung der

---

[77] BVerfGE 141, 220 (272); 165, 363 (411); BVerfG, NVwZ 2024, 1736 (1742).

[78] Vgl. Bäuerle, in: BeckOK PolR Hessen, 33. Ed. 1.6.2024, HSOG § 25a Rn. 35.

[79] Vgl. Ruschemeier, Predictive Policing, in: Ebers (Hrsg.), StichwortKommentar Legal Tech, 2024, Rn. 10b.

[80] Vgl. BVerfGE 165, 363 (438).

Eingriffsvoraussetzungen auch an die Begehungsgefahr von Vorfeldtatbeständen anzuknüpfen. Er muss jedoch in jedem Einzelfall sicherstellen, dass eine konkrete oder konkretisierte Gefahr für die durch den Straftatbestand geschützten Rechtsgüter besteht. Knüpft der Gesetzgeber an die Begehung solcher Straftaten an, muss er daher **zusätzlich verlangen, dass bereits eine konkretisierte oder konkrete Gefahr für das geschützte Rechtsgut vorliegt**.[81] Daran fehlt es hier. Somit ist diese Ermächtigungsgrundlage ohne entsprechende Änderung ebenfalls **verfassungswidrig**.[82]

(4) Datenanalyse gemäß § 30a Abs. 7 SOG LSA

Gemäß § 30a Abs. 7 S. 1 SOG LSA kann die Polizei auf einer Analyseplattform gespeicherte personenbezogene Daten, wenn dies für eine bestimmte strategische Datenanalyse erforderlich ist, weiterverarbeiten, soweit eine Weiterverarbeitung anonymisierter Daten zu diesem Zweck nicht möglich ist und das öffentliche Interesse an der strategischen Datenanalyse das schutzwürdige Interesse der betroffenen Personen erheblich überwiegt.

Damit unterscheiden sich die Voraussetzungen einer strategischen Datenanalyse deutlich von den Voraussetzungen einer operativen Datenanalyse (siehe zuvor). Statt dem Erfordernis einer zumindest hinreichend konkretisierten Gefahr für besonders gewichtige Rechtsgüter reichen für eine strategische Datenanalyse die Unmöglichkeit einer Weiterverarbeitung anonymer Daten und das erhebliche Überwiegen öffentlicher Interessen aus. Wären an strategische Datenanalysen ebenfalls die engen Rechtfertigungsanforderungen eingriffsintensiver heimlicher Überwachungsmaßnahmen anzulegen, wäre die vorgeschlagene Ermächtigungsgrundlage folglich eklatant verfassungswidrig. § 30a Abs. 7 SOG LSA zielt jedoch – wie sich aus § 30a Abs. 2 SOG LSA ergibt – auf nicht personenbezogene Maßnahmen, sodass **eine niedrigere Eingriffsschwelle** zulässig ist. Außerdem hat der Gesetzgeber eine technische Maßnahme ergriffen, um den Bezug der Daten zu natürlichen Personen zu erschweren. Gemäß § 30a Abs. 7 S. 2 SOG LSA sind die personenbezogenen Daten zu pseudonymisieren.

---

[81] BVerfGE 165, 363 (439).

[82] Vgl. Bäuerle, in: BeckOK PolR Hessen, 33. Ed. 1.6.2024, HSOG § 25a Rn. 39; Ruschemeier, Predictive Policing, in: Ebers (Hrsg.), StichwortKommentar Legal Tech, 2024, Rn. 10b.

Dennoch muss auch § 30a Abs. 7 S. 1 SOG LSA den **Grundsatz der Zweckbindung** wahren. Zweckänderungen sind stets an den Grundrechten zu messen, die für die ursprüngliche Datenerhebung maßgeblich waren.[83] Dabei orientiert sich das Gewicht einer solchen Regelung i.R.d. Abwägung am Umfang des Eingriffs bei der Datenerhebung. Informationen, die durch besonders eingriffsintensive Maßnahmen gewonnen wurden, dürfen auch nur für besonders gewichtige Zwecke verwendet werden. Als Maßstab für die Verhältnismäßigkeitsprüfung dient in diesem Zusammenhang das **Kriterium der hypothetischen Datenneuerhebung**.[84] Der Gesetzgeber kann eine Zweckänderung der Daten im Hinblick auf die Nutzung durch Sicherheitsbehörden grundsätzlich dann zulassen, wenn es sich um Informationen handelt, aus denen sich im Einzelfall konkrete Ermittlungsansätze zur Aufdeckung von vergleichbar gewichtigen Straftaten oder zur Abwehr von zumindest auf mittlere Sicht drohenden Gefahren für vergleichbar gewichtige Rechtsgüter wie die ergeben, zu deren Schutz die entsprechende Datenerhebung zulässig ist.[85] Diese Anforderungen sichert § 30a Abs. 7 S. 1 SOG LSA bislang nicht ausdrücklich ab. Es sollte daher zumindest klarstellend auf **§ 13b SOG LSA** verwiesen werden. Praktisch dürfte zudem eine **Kennzeichnung von Daten** erforderlich sein, um die Einhaltung der verfassungsrechtlichen Vorgaben überprüfen zu können.[86] Aus § 30a Abs. 8 Nr. 3 SOG LSA lässt sich indes schließen, dass der Entwurf bislang keine neuen Kennzeichnungen bezweckt.

(5) Fehlendes Kontrollkonzept

Der Verhältnismäßigkeitsgrundsatz stellt auch Anforderungen an Transparenz, individuellen Rechtsschutz und aufsichtliche Kontrolle.[87] Entscheidend ist dabei eine **sachgerechte Ausgestaltung der Kontrolle**. Um der möglicherweise hohen Zahl von Maßnahmen Herr zu werden, sind sowohl ein abgestuftes Kontrollkonzept zwischen unabhängigen und behördlichen Datenschutzbeauftragten

[83] BVerfGE 165, 363 (393).

[84] BVerfGE 165, 363 (393).

[85] BVerfGE 165, 363 (393).

[86] Vgl. BVerfGE 165, 363 (395).

[87] stRspr. des BVerfG, siehe BVerfGE 141, 220 (282) m.w.N.

als auch ein stichprobenartiges Vorgehen zulässig.[88] Die aufsichtlichen Kontrollen sind dabei **regelmäßig durchzuführen** (mindestens alle zwei Jahre), damit sie ihrer Kompensationsfunktion für den schwach ausgestalteten Individualrechtsschutz gerecht werden können (vgl. z.B. § 69 Abs. 1 BKAG).[89] Gemessen an diesen Anforderungen begründet § 30a SOG LSA kein ausreichendes Kontrollkonzept. In der Norm selbst ist lediglich festgehalten, dass § 24 Abs. 3 DSAG LSA Anwendung findet (§ 30a Abs. 3 S. 2 SOG LSA). Daraus folgt aber nur eine Unterrichtungspflicht bzw. ein Anhörungsrecht der Landesbeauftragten für den Datenschutz vor der Einrichtung einer Analyseplattform und **keine speziellen Kontrollpflichten während des Plattformbetriebs**. Diese folgen auch nicht aus anderen Vorgaben des allgemeinen Datenschutzrechts, das nur Kontrollrechte begründet. Ohne Kontrollpflichten kann der Gesetzgeber aber keine Regelmäßigkeit der aufsichtlichen Kontrollen sicherstellen. Der behördliche Datenschutzbeauftragte findet im aktuellen Gesetzentwurf gar keine Berücksichtigung (vgl. hingegen bspw. § 25a Abs. 4 S. 6 HSOG: „Die oder der behördliche Datenschutzbeauftragte ist zur Durchführung stichprobenartiger Kontrollen berechtigt.“).

3. Fazit

Die aus § 30a SOG LSA folgenden Grundrechtseingriffe sind unangemessen und damit unverhältnismäßig. Die **Norm verstößt im gegenwärtigen Entwurfsstadium gegen das Recht auf informationelle Selbstbestimmung** (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG), da insbesondere die Ermächtigungsgrundlagen des § 30a Abs. 6 Nr. 2 und Nr. 3 SOG LSA keine angemessene Eingriffsschwelle vorsehen, die dem Gewicht des mit diesen Maßnahmen verbundenen Eingriffs gerecht wird und weil die gesamte Norm über kein ausreichendes Kontrollkonzept verfügt.

[88] BVerfGE 165, 363 (412).

[89] BVerfGE 141, 220 (285).

II. Unionskonformität

Eine automatisierte Datenanalyse ruft neben dem nationalen Verfassungsrecht auch das Unionsrecht auf den Plan. Dem steht nicht entgegen, dass dem Unionsgesetzgeber im Bereich der **nationalen Sicherheit** keine Regelungsbefugnis zukommt (Art. 4 Abs. 2 EUV). Denn nach dem EuGH ist die nationale Sicherheit von der öffentlichen Sicherheit abzugrenzen und umfasst nur die Sicherheit bzw. den Bestand des Staates selbst (z.B. vor terroristischen Aktivitäten).[90]

1. Datenschutzrecht

Vorrangiger Rechtsrahmen für eine automatisierte Datenanalyse ist das unionale Datenschutzrecht, wie es sich aus der Richtlinie (EU) 2016/680 (JI-RL) ergibt und u.a. mit dem DSUG LSA in mitgliedstaatliches Recht umgesetzt worden ist. Daher ist bspw. vor der Einführung einer Analyseplattform i.S.d. § 30a SOG LSA zwingend eine **Datenschutz-Folgenabschätzung** vorzunehmen (Art. 27 JI-RL bzw. § 23 DSUG LSA).

2. KI-Recht

Zusätzlich ist die Verordnung über künstliche Intelligenz (KI-VO) zu beachten, da auf Grundlage von § 30a SOG LSA auch KI-Systeme zum Einsatz kommen können (siehe oben C. I. 2. c) aa) (2) (a)). Sie ist 2024 in Kraft getreten und gilt auch für öffentliche Stellen der Mitgliedstaaten wie die Polizei unmittelbar. Für den KI-Begriff des Art. 3 Nr. 1 KI-VO kommt es nicht darauf an, dass das System selbstlernend ist.[91]

Die KI-VO **verbietet** den Einsatz bestimmter KI-Systeme generell. Im Kontext von § 30a SOG LSA ist dabei von Relevanz, dass zu den verbotenen KI-Praktiken (zumindest in Teilen) auch **personenbezogenes Predictive Policing** zählt. Konkret untersagt ist das Inverkehrbringen, die Inbetriebnahme für diesen spezifischen Zweck oder die Verwendung eines KI-Systems zur

[90] EuGH, CR 2008, 381 (382); Botta, CR 2020, 82 (85); Pilniok, DÖV 2024, 581 (584).

[91] Wendehorst, in: Martini/Wendehorst (Hrsg.), KI-VO, 2024, Art. 3 Rn. 32 ff.; vgl. Benamor, BayVBl 2025, 44 (48 f.).

Durchführung von Risikobewertungen in Bezug auf natürliche Personen, um das Risiko, dass eine natürliche Person eine Straftat begeht, ausschließlich auf der Grundlage des Profiling einer natürlichen Person oder der Bewertung ihrer persönlichen Merkmale und Eigenschaften zu bewerten oder vorherzusagen (Art. 5 Abs. 1 lit. d Hs. 1 KI-VO). Die Polizei darf folglich auf Grundlage von § 30a SOG LSA keine Software verwenden, die entsprechend zum Einsatz kommt. Das Verbot gilt indes nicht für KI-Systeme, die dazu verwendet werden, die durch Menschen durchgeführte Bewertung der Beteiligung einer Person an einer kriminellen Aktivität, die sich bereits auf objektive und überprüfbare Tatsachen stützt, die in unmittelbarem Zusammenhang mit einer kriminellen Aktivität stehen, zu unterstützen (Art. 5 Abs. 1 lit. d Hs. 2 KI-VO).

Sind polizeiliche KI-Systeme nicht durch Art. 5 KI-VO verboten, stellt es sie jedoch nicht per se von den Vorgaben der Verordnung frei. Diese richten sich nämlich vornehmlich an sogenannte **Hochrisiko-KI-Systeme** (d.h. an deren Anbieter oder Betreiber i.S.d. Art. 3 KI-VO). Ob ein KI-System als Hochrisiko-KI-System zu bewerten ist, bestimmt sich insbesondere nach Annex III KI-VO. Daraus ergibt sich, dass der polizeiliche KI-Einsatz nicht pauschal als hochriskant gilt. Vielmehr muss ein polizeilich verwendetes KI-System den abschließend genannten Kategorien von Hochrisiko-KI-Systemen unterfallen. Im Kontext von § 30a SOG LSA dürfte vor allem eine Kategorie von Hochrisiko-KI-Systemen relevant sein. Dies sind KI-Systeme, die zur Wahrscheinlichkeitsbewertung der Begehung von Straftaten (soweit diese Risikobewertung nicht nur auf der Grundlage von Persönlichkeitsprofilen gemäß Art. 3 Abs. 4 JI-RL erfolgt) oder zur Bewertung persönlicher Merkmale und Eigenschaften oder vergangenen kriminellen Verhaltens von natürlichen Personen oder Gruppen verwendet werden sollen (Annex III Nr. 6 lit. d KI-VO). Ist eine polizeilich verwendete Software als Hochrisiko-KI-System einzustufen, sind die umfassenden (produktsicherheitsrechtlichen) Pflichten der Art. 6 ff. KI-VO zu beachten.[92] Unter anderem müssen die Polizeibehörden die entwickelten oder verwendeten KI-Systeme in der EU-Datenbank gemäß Art. 71 KI-VO registrieren.

[92] Bäuerle, ZD 2025, 128 (131).

III. Technische Umsetzung

Auch wenn § 30a SOG LSA technikneutral ausgestaltet ist (siehe oben C. I. 2. c) aa) (2) (a)), lässt sich die Norm nicht gänzlich losgelöst von ihrer technischen Umsetzung bewerten. Ausweislich dem Gesetzentwurf soll eine Software zum Einsatz kommen, über die sich Bund und Länder bereits abgestimmt haben.[93] Dabei dürfte es sich um die Software **„Gotham" des US-amerikanischen Unternehmens Palantir Technologies GmbH** handeln. Das Bayerische Landeskriminalamt hat in einem europaweiten Vergabeverfahren für eine polizeiliche verfahrensübergreifende Recherche- und Analysesoftware Palantir den Zuschlag erteilt.[94] Aus dem geschlossenen Mantelrahmenvertrag sind die Länder und der Bund i.R.d. Programms „Polizei 20/20" selbständig abrufberechtigt. Derzeit kommt „Gotham" (unter anderem Namen) bereits in Bayern (VeRA), Hessen (HessenDATA) und NRW (DAR) zum Einsatz.[95]

Im Jahr 2023 hat die Bundesinnenministerin Nancy Faeser (SPD) jedoch entschieden, dass das Bundeskriminalamt und die Bundespolizei die Software nicht nutzen dürfen.[96] Stattdessen hat sich das Bundesministerium des Innern für eine **herstellerunabhängige Entwicklung** entschieden.[97] Aus Gründen der **digitalen Souveränität** sollte auch das Land Sachsen-Anhalt dringend prüfen, ob es die Monopolstellung von Palantir weiter stärken oder sich der Bundesinitiative anschließen will. Insbesondere das Kostenargument gegen eine herstellerunabhängige Entwicklung verfängt nur begrenzt, da auch die Nutzungskosten privater Software erheblich sind.[98] Sollte sich abzeichnen, dass

[93] LT-Drs. 8/5018, S. 5.

[94] Benamor, BayVBl 2025, 44 (45).

[95] Bäuerle, ZD 2025, 128 (128).

[96] BT-Drs. 20/8390, S. 2.

[97] BT-Drs. 20/8390, S. 5.

[98] Ruf, Stellungnahme zu dem Antrag der Fraktion der CDU/CSU „Handlungsfähigkeit der Strafverfolgungsbehörden sichern – Entscheidung des Bundesministeriums des Innern und für Heimat bezüglich der polizeilichen Analyse-Software Bundes-VeRA revidieren" (BT-Drs. 20/9495), Ausschuss-Drs. 20(4)418 D, S. 10.

§ 30a SOG LSA letztendlich nur „Gotham“ legalisieren soll, ist im Normtext zwingend ein ausreichendes **staatliches Monitoring** der Software abzusichern.[99]

D. Fazit

Die Landesregierung hat zu Recht die Notwendigkeit erkannt, die Gefahrenabwehr an die Herausforderungen des 21. Jahrhunderts anzupassen. Damit dieses Ziel erreicht werden kann, sind nicht nur rechtliche und technische Neuerungen erforderlich, sondern auch eine sorgfältige **Beachtung des Verfassungs- und Unionsrechts**. Der gegenwärtige Gesetzentwurf erfüllt diese Anforderung bislang noch nicht ausreichend. Daher liegt es nun in der Verantwortung des Landtages, die rechtlichen Grundlagen für die automatisierte Kennzeichenkontrolle sowie insbesondere die automatisierte Datenanalyse entsprechend nachzubessern. Sollte er dies unterlassen, riskierte er, verfassungswidriges Recht zu schaffen. In einem solchen Fall wären eine Verfassungsbeschwerde, wie sie bereits gegen den reformierten § 25a HSOG erhoben worden ist,[100] und ein neues Urteil zum polizeilichen Data-Mining wohl nicht unwahrscheinlich. Es ist jedoch entschieden **als Fehlentwicklung zu kritisieren, wenn die Legislative die Fortschreibung des Sicherheitsrechts immer mehr dem BVerfG überlässt** und sich überwiegend darauf beschränkt, die von Karlsruhe aufgezeigten Grenzen (nachträglich) in den Normtext zu übernehmen. Damit steht der Gesetzgeber in Sachsen-Anhalt freilich vor Herausforderungen, die auch schon in anderen Ländern und im Bund aufgetreten sind oder noch auftreten werden. Es zeigt sich (nicht nur) vor diesem Hintergrund, dass insbesondere im Bereich der digitalen Gefahrenabwehr ein **einheitliches Musterpolizeigesetz**[101] fehlt. Perspektivisch sollte das Land Sachsen-Anhalt daher aktiv auf die Schaffung eines derartigen Regelungsentwurfs hinwirken.

---

[99] Vgl. BVerfGE 165, 363 (412 f.); Ruschemeier, Predictive Policing, in: Ebers (Hrsg.), StichwortKommentar Legal Tech, 2024, Rn. 10d; Santhakumar, „Legal Design“ für HessenData (§ 25a HSOG) – ein abgestuftes Kontrollkonzept, in: Botta et al. (Hrsg.), Rechtsfragen virtueller Welten, 2025, S. 103 (114 f.).

[100] Online abrufbar unter: https://freiheitsrechte.org/uploads/documents/Freiheit-im-digitalen-Zeitalter/Polizeigesetz-Hessen/Verfassungsbeschwerdeschrift-HSOG.pdf.

[101] Dazu z.B. Aden/Fährmann, Polizeirecht vereinheitlichen? Kriterien für Muster-Polizeigesetze aus rechtsstaatlicher und bürgerrechtlicher Perspektive, 2018.