Gesellschaft für Freiheitsrechte

freiheitsrechte.org

7. Mai 2025

Stellungnahme

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

Von Franziska Görlitz

Volljuristin und Verfahrenskoordinatorin bei der Gesellschaft für Freiheitsrechte e.V.

Der Gesetzesentwurf dient der Verlängerung der Höchstdauer des Präventivgewahrsams für terroristische Gefährder*innen sowie der Schaffung von Befugnissen zur Durchführung automatisierter Kennzeichenerfassungen und automatisierter Datenanalysen. Darüber hinaus soll der Schutz von Opfern und potenziellen Opfern häuslicher Gewalt verbessert werden. Die vorliegende Stellungnahme beschränkt sich auf den Entwurf einer Rechtsgrundlage für eine automatisierte Datenanalyse in § 30a des Entwurfes und dessen Vereinbarkeit mit verfassungsrechtlichen Vorgaben.

§ 30a des Entwurfes schafft eine Rechtsgrundlage für zwei Formen der automatisierten Datenanalyse: eine operative Datenanalyse für die einzelfallbezogene Analyse personenbezogener Daten für Strafverfolgung, Gefahrenabwehr und Verhinderung von Straftaten (Abs. 1, 6) und eine strategische Datenanalyse, mit der neben anonymisierten auch personenbezogene Daten für insbesondere die Ermittlung von gefährdeten und gefährlichen Orten, Kriminalitätsphänomenen, Tätergruppierungen sowie statistische Zwecke analysiert werden können (Abs. 2, 7).

Zusammenfassung:

Der vorliegende Entwurf setzt die Maßstäbe des Bundesverfassungsgerichts aus der Entscheidung des Bundesverfassungsgerichts vom 16. Februar 2023 (1 BvR 1547/19, 1 BvR 2634/20) nicht hinreichend um. Bei der vorgesehenen operativen Datenanalyse handelt es sich um einen schwerwiegenden Grundrechtseingriff, da die gesetzlichen Einschränkungen der Datenanalyse nicht ausreichend sind, um das Eingriffsgewicht maßgeblich zu reduzieren. Zudem enthält § 30a Abs. 6 Nr. 3 des Entwurfs eine unzulässige dynamische Verweisung auf §§ 100a f. StPO. Auch die

strategische Datenanalyse stellt keinen nur geringfügigen Grundrechtseingriff dar, sodass die vom Bundesverfassungsgericht entwickelten Anforderungen an eine Rechtfertigung nicht gewahrt sind. Weiterhin ist die Einhaltung der Grundsätze der Zweckbindung und Zweckänderung nicht ausreichend sichergestellt. Es fehlen hinreichende datenschutzrechtliche Kontrollmechanismen sowie Vorkehrungen gegen Diskriminierung und zur Erkennung und Vermeidung von Fehlern. Der Entwurf genügt insgesamt dem Gesetzesvorbehalt und dem Wesentlichkeitsgrundsatz sowie den Anforderungen an Bestimmtheit und Normenklarheit nicht, da für grundrechtswesentliche Bereiche die durch den Gesetzgeber vorzunehmenden Abwägungen an den Verordnungsgeber ausgelagert werden. Dies betrifft Regelungen zu Art und Umfang der zusammengeführten Daten, Einschränkungen der Zugriffsberechtigung, Kennzeichnungsverpflichtungen und Sicherstellung der Zweckbindung, sowie zu Methoden der Datenanalyse und Protokollierung und Dokumentation der Analysevorgänge.

Rechtliche Bewertung der Regelungen im Einzelnen

A. Verfassungsrechtlicher Maßstab

Datenzusammenführungen und Datenverarbeitungen auf Grundlage bereits erhobener personenbezogener Informationen stellen selbstständige Eingriffe in das Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) dar und bedürfen daher einer spezifischen Ermächtigungsgrundlage.[1] Dabei hängen die Anforderungen an die verfassungsrechtliche Rechtfertigung[2], die sich in der Rechtsgrundlage widerspiegeln müssen, von der Eingriffsintensität unter Berücksichtigung der Wesentlichkeitstheorie und den Grundsätzen der Bestimmtheit und Normenklarheit ab.

Maßgeblich für die Eingriffsintensität sind insbesondere Art und Umfang der verarbeiteten Daten sowie die konkrete Methode der Auswertung.[3] Je umfangreicher und sensibler die verwendeten Daten, je komplexer, weitreichender und intransparenter die eingesetzte Analysemethode und je größer die daraus resultierende Missbrauchsgefahr, desto schwerer ist das Eigengewicht des Eingriffs.[4] Hiermit korrespondiert ein gestuftes Modell der Rechtfertigungsanforderungen[5]:

Besonders schwerwiegende Grundrechtseingriffe sind nur unter den engen Voraussetzungen zu rechtfertigen, die das Bundesverfassungsgericht allgemein für eingriffsintensive heimliche Überwachungsmaßnahmen entwickelt hat.[6] Derartige Maßnahmen sind nur im Falle einer

1 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 50 f.
2 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 51, 72 ff.
3 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 75 ff.
4 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 76 ff.
5 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 71 ff.
6 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 104 ff.

zumindest hinreichend konkretisierten Gefahr für besonders gewichtige Rechtsgüter wie Leib, Leben oder Bestand des Staates zulässig.[7] Weniger eingriffsintensive Maßnahmen unterliegen abgestuften Anforderungen: Sie können entweder bei einer konkretisierten Gefahr für zumindest erhebliche Rechtsgüter oder bei einer noch nicht konkretisierten Gefahr im Vorfeld zum Schutz hochrangiger, überragend wichtiger oder auch besonders gewichtiger Rechtsgüter gerechtfertigt sein.[8] Lediglich bei nur geringfügigen Eingriffen – etwa bei einem automatisierten Datenabgleich, der in Ablauf und Verarbeitungsergebnis mit einem händischen Abgleich vergleichbar ist – genügt die Wahrung des Grundsatzes der Zweckbindung für eine Rechtfertigung.[9]

Das Bundesverfassungsgericht hebt darüber hinaus die verfassungsrechtlichen Anforderungen an den Gesetzesvorbehalt und den Wesentlichkeitsgrundsatz hervor.[10] Für grundrechtswesentliche Entscheidungen – insbesondere solche über die Begrenzung der Art und Menge der Daten, die Wahl der zulässigen Auswertungsmethoden, die Einbeziehung technischer Systeme sowie Regelungen zur Dokumentation, Kontrolle und Nachvollziehbarkeit – muss der Gesetzgeber entsprechend dem Gesetzesvorbehalt die grundrechtswesentlichen Entscheidungen selbst treffen.[11] Zwar kann der Gesetzgeber Ermächtigungen zur Ausgestaltung technischer und organisatorischer Einzelheiten an die Verwaltung delegieren, die grundlegenden Einschränkungen müssen jedoch durch Gesetz geregelt oder hinreichend bestimmt gesetzlich vorgesehen sein.[12] Je höher die Eingriffsintensität, desto höher sind hierbei die Anforderungen an Bestimmtheit[13] und Normenklarheit, die sowohl inhaltliche Verständlichkeit und Vorhersehbarkeit der Eingriffsbefugnisse[14] als auch effektive gerichtliche Kontrolle gewährleisten sollen.[15]

B. Wahrung dieser Grundsätze

I. Eingriffsgewicht der Maßnahmen

1. Operative Datenanalyse

In der vorliegenden Fassung stellt die operative Datenanalyse einen **schwerwiegenden Grundrechtseingriff** dar, sodass die im Entwurf vorgesehenen Eingriffsschwellen und die zu schützenden Rechtsgüter zur Rechtfertigung des Eingriffs nicht genügen. Das Eingriffsgewicht der

---

7 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 104 ff.
8 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 107.
9 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 108.
10 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 110.
11 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 110, 112 ff.
12 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 112 ff.
13 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 115, 120.
14 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 110, 114.
15 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 109.

operativen Datenanalyse ist **mangels ausreichend bestimmter und normenklarer Einschränkung** durch den Gesetzgeber selbst nicht ausreichend gemildert.

a. Art und Umfang der Daten

Der vorliegende Entwurf begrenzt weder Art noch Umfang der Daten ausreichend.

In die Analyse dürfen gemäß § 30a Abs. 4 S. 2 des Entwurfs mit Vorgangsdaten, Falldaten und Verkehrsdaten umfangreiche und teils noch nicht fachlich beurteilte Datensätze in die Analyse eingeführt werden. Diese enthalten zu erheblichem Teil auch Daten von Personen, die keinen Anlass dafür geboten haben, einer Maßnahme durch die Datenanalyse ausgesetzt zu werden. Dies gilt insbesondere für die explizit aufgenommenen Telekommunikationsdaten und Daten aus Funkzellenabfragen.

Eingeführt werden dürfen diese Daten bezüglich der in § 30a Abs. 4 S. 1 genannten Personen. Die dort aufgeführten Verweise begrenzen die Datenmenge jedoch unzureichend. Insbesondere können über § 30a Abs. 4 S. 1 Nr. 2 des Entwurfs i.V.m. § 15 Abs. 2 Nr. 2 und 3 SOG LSA Kontaktpersonen und gefährdete Personen, die sich im räumlichen Umfeld von Gefährdungspersonen aufhalten, umfasst sein. Noch weitergehend sind über § 30a Abs. 4 S. 1 Nr. 7 des Entwurfs i.V.m. § 23 Abs. 6, 7, 8 SOG LSA auch Daten von Zeug*innen, Opfern, Kontaktpersonen, Hinweisgeber*innen und anderen Auskunftspersonen, sowie Vermissten, unbekannten Personen und unbekannten Toten umfasst, ebenso Daten von Personen, bei denen festgestellt werden soll, ob sie diese Voraussetzungen erfüllen. Der Personenkreis umfasst also einen **hohen Anteil von Personen**, die **keinen Anlass für gegen sie gerichtete Analysemaßnahmen gegeben** haben. Auch sieht die Norm keinen Schutz für besonders schützenswerte Kontaktpersonen wie Anwält*innen und Journalist*innen vor, die besondere Gefahr laufen, dass ihre Daten in die Analyse eingebunden werden.

Die Analyseplattform darf zwar gemäß § 30a Abs. 4 S. 4 des Entwurfs nicht direkt mit dem Internet verbunden werden. Gleichzeitig ist es aber möglich, Daten aus dem Internet, insbesondere Informationen aus sozialen Medien und aus anderen staatlichen Registern noch in die Analyse einzuführen, § 30a Abs. 4 S. 3. Der Entwurf enthält keine Regelungen, ob auf diese Weise zugeführte Daten in der Analyseplattform verbleiben oder wieder entfernt werden.

Als einzige explizite Einschränkung nimmt § 30a Abs. 4 S. 5 personenbezogene Daten aus Wohnraumüberwachungen und Onlinedurchsuchungen aus, wie es vom Bundesverfassungsgericht für die in Abs. 6 vorgesehenen Gefahrenschwellen vorgegeben ist.[16] Daten aus anderen schwerwiegenden Grundrechtseingriffen wie u.a. dem Einsatz verdeckter Ermittler*innen und Vertrauenspersonen, längerfristigen Observationen, Telekommunikationsüberwachungen und

[16] BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 81.

Verkehrsdatenabfragen[17] sind nicht ausgenommen, Telekommunikationsdaten und Daten aus Funkzellenabfragen sind vielmehr explizit in § 30a Abs. 4 S. 2 des Entwurfs erwähnt.

Darüber hinaus sieht der Entwurf **weder eine Beschränkung auf nur polizeilich erhobene Daten noch eine Beschränkung auf nur durch das Land Sachsen-Anhalt oder nur inländische Behörden erhobene Daten** vor. Insbesondere durch die in § 30a Abs. 4 S. 2 des Entwurfs genannten Informationssysteme der Polizei, dem polizeilichen Informationssystem zwischen Bund und den Ländern und dem polizeilichen Informationsaustausch können auch Daten von inländischen oder ausländischen Nachrichtendiensten in die Analyse eingebunden werden.

Die Menge der umfassten Daten wird ebenfalls nicht dadurch eingeschränkt, dass nur Daten zu näher eingegrenzten Straftaten aufgenommen werden dürfen. Zudem können Daten nicht nur rein händisch hinzugezogen, sondern automatisiert zusammengeführt werden. Ebenso sieht das Gesetz selbst keine Zugangsbeschränkung zu der Analysesoftware sowie keine ausreichende Sicherung der Grundsätze der Zweckbindung und Zweckänderung vor (hierzu sogleich unter c. und e.).

Hinsichtlich der Art der Daten enthält der Entwurf auch insoweit keine Einschränkungen, dass besonders sensible Daten wie biometrische Daten, Screenshots von Kommunikationen, Bilder und Videos einbezogen werden können. Zudem enthält die Norm keine tatsächlichen Einschränkungen zum Schutz von besonders diskriminierungssensiblen Daten.

b. Methode der Datenanalyse

Auch die Methoden der Datenanalysen sind weit und durch den Entwurf nur unzureichend eingeschränkt. Zwar ist zu begrüßen, dass die erlaubten Methoden in § 30a Abs. 5 S. 1 des Entwurfs abschließend aufgezählt sind. Jedoch umfasst diese Aufzählung u.a. Methoden wie „Data-Mining, maschinelles Lernen, Data Science und Sekundärdatenanalyse". Diese Begriffe sind **technisch weit**, die Methoden daher **nicht ausreichend bestimmt**. § 30a Abs. 5 des Entwurfs ermöglicht damit insbesondere den Einsatz von starken und komplexen Analysesystemen, die auch zu maschineller Sachverhaltsbewertung in der Lage sind und in kürzester Zeit komplexe Ergebnisse hervorbringen können. § 30a Abs. 5 des Entwurfs ermöglicht mit den genannten Methoden zudem den Einsatz künstlicher Intelligenz, deren Einsatz ein besonderes Eingriffsgewicht zukommt.[18] Dass die analysierten Daten nach der Gesetzesbegründung (2.1.13 am Ende, S. 57 des Entwurfs) nicht dazu genutzt werden dürfen, KI-Systeme anzulernen, ändert hieran nichts, zumal diese Beschränkung nicht wie erforderlich[19] in den Gesetzestext aufgenommen wurde.

---

17 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 176.
18 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 100.
19 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 121.

Auch ist die methodische Bedien- und Arbeitsweise der Analyse kaum geregelt. Zwar wird die Analyse gemäß § 30a Abs. 3 S. 3 des Entwurfs manuell ausgelöst. Sie verläuft dann jedoch entweder regelbasiert oder nach den Methoden und Techniken des Abs. 5. Daher sind weder die Anzahl oder Art der Analyseschritte und -verknüpfungen begrenzt, noch ist die Analyse auf den Einsatz von Suchbegriffen beschränkt. Es besteht gemäß § 30a Abs. 4 S. 3 des Entwurfs vielmehr die Möglichkeit, immer wieder neue Daten in die Analyse hinzuzufügen und endlose Analysevorgänge durchzuführen. Dass die operative Datenanalyse gemäß § 30a Abs. 1 S. 1 des Entwurfs „im Einzelfall" erfolgt, stellt keine ausreichende Begrenzung dar. Auch ein Einzelfall kann zum Anlass für weitgehende Analysemaßnahmen genommen werden und so bei Zielpersonen, aber auch Dritten erhebliche Grundrechtseingriffe zur Folge haben.

Die zugelassenen Methoden ermöglichen so mangels gesetzlichen Ausschlusses auch die Erstellung von **Personen- und Bewegungsprofilen sowie die Bewertung von Personen und Gefährdungen bzw. Risiken in Form des „predictive policings"** und damit **besonderes intensive Grundrechtseingriffe.**[20] Sie unterscheiden sich erheblich von einem bloß maschinellen Datenabgleich, gerade weil sie explizit darauf gerichtet sind, neues Wissen zu erzeugen (2.1.13, S. 57 des Entwurfs).

Ebenso verstärkt das Eingriffsgewicht, dass § 30a Abs. 4 S. 1 des Entwurfs es ermöglicht und darauf zielt, die Daten nicht nur vorübergehend für einen konkreten Verarbeitungsvorgang, sondern dauerhaft in einer eigenen Datenbank zusammenzuführen und so für die Analyseplattform als Datenbestand zur Verfügung zu stellen (2.1.13, S. 58 des Entwurfs).

Die einsetzbaren Methoden sind im Entwurf daher nicht ausreichend bestimmt und normenklar begrenzt. Selbst wenn die Datenverarbeitung praktisch weniger eingriffsintensiv ausgestaltet wäre, bliebe dies für das Eingriffsgewicht der Ermächtigung zur Datenverarbeitung ohne Bedeutung. Entscheidend sind vielmehr die Möglichkeiten, die der Gesetzgeber mangels Einschränkungen durch seine Rechtsgrundlage eröffnet.

c. Unzureichende Sicherung des Grundsatzes der Zweckbindung

Der Entwurf sieht keine explizite Inbezugnahme der Zweckbindungsvorschriften des SOG LSA, insbesondere von § 13b vor. Lediglich enthält § 30a Abs. 8 Nr. 3 und 4 des Entwurfs Verordnungsermächtigungen zur Regelung der Aufrechterhaltung bestehender Kennzeichnungen zur Sicherung der Einhaltung der Zweckbindung sowie der sonstigen technischen Vorkehrungen zur Sicherstellung der Beachtung von § 13b. Gerade für die strategische Datenanalyse bedarf es einer **expliziten gesetzlichen Klarstellung**, dass die gesetzlichen Zweckbindungsregelungen unberührt bleiben.

---

[20] BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 98, 121.

Darüber hinaus stellen die vorgesehenen Regelungen zur Kennzeichnung der zusammengeführten Daten in § 30a Abs. 4 S. 6 des Entwurfs die Einhaltung des Grundsatzes der Zweckbindung nicht ausreichend sicher. Allein rechtliche Vorgaben zur Zweckbindung können bei einer automatisierten Datenzusammenführung großer Datenmengen die tatsächliche Wahrung der Zweckbindungsgrundsätze nicht sichern, da in großen, unübersehbaren Datenpools und bei teils automatisierter Einbindung eine Zweckidentifizierung und -prüfung für einzelne Daten erschwert wird.[21] Damit die Zweckbindung und -änderung in der praktischen Anwendung tatsächlich geprüft und gewahrt werden kann, bedarf es vielmehr auch einer **faktischen Sicherung der Zweckbindung.**

In der Entwurfsfassung des § 30a wird die Zweckbindung nicht dadurch gesichert, dass die verarbeiteten Datenquellen bzw. -sätze nach Zwecken getrennt bleiben. Vielmehr sollen die verschiedenen Datensätze für die Analyse dauerhaft zusammengeführt und verfügbar gemacht werden.

Daher bedarf es zur Sicherung der Zweckbindung insbesondere einer **umfassenden Kennzeichnung** von Daten.[22] Die im Entwurf enthaltene Regelung sieht jedoch nur vor, dass bereits bestehende Kennzeichnungen aufrechtzuerhalten sind. Es ist mithin nicht ausgeschlossen, dass in Datensätzen befindliche nicht gekennzeichnete Daten dennoch zu anderen nicht zulässigen Zwecken in Analysevorgänge einfließen können. Insoweit sollte § 13d Abs. 2 SOG LSA in Bezug genommen werden. Ohnehin kann aber allein eine Kennzeichnung der verwendeten Daten nicht dafür sorgen, dass die durch Zweckbindungsregelungen gesetzten Grenzen für die einzelnen Daten eingehalten werden.[23]

d. Unzureichende aufsichtliche Kontrolle

Der Entwurf sieht zudem keine ausreichende aufsichtliche, insbesondere datenschutzrechtliche Kontrolle vor, wie sie zur Wahrung des Verhältnismäßigkeitsgrundsatzes erforderlich ist. § 30a Abs. 3 S. 2 des Entwurfs sieht lediglich einen Verweis auf § 23 Abs. 3 des Datenschutz-Grundverordnungs-Ausfüllungsgesetz Sachsen-Anhalt vor. Dieser regelt jedoch nur eine Unterrichtung und Anhörung des*r Datenschutzbeauftragten vor der Einrichtung der Analyseplattform. Als mögliche sachgerechte Ausgestaltung einer verfassungsrechtlich gebotenen Kontrolle kommt nach dem Bundesverfassungsgericht etwa eine **regelmäßige und effiziente stichprobenhafte Kontrolle des Analysebetriebs** durch behördliche und externe Datenschutzbeauftragte in Betracht.[24] Die Kontrollzeiträume dürfen dabei ein Höchstmaß von etwa zwei Jahren nicht überschreiten.[25] Gerade zu Beginn der Nutzung der operativen und strategischen

---

21 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 138.
22 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 65.
23 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 139.
24 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 109.
25 BVerfG, Urteil vom 20. April 2016, 1 BvR 966, 1140/09, Rn. 141.

Datenanalyse ist eine externe Kontrolle zum Ausschluss von Fehlern, Diskriminierung und Missbrauch in geringeren Abständen notwendig. Eine solche Kontrolle oder vergleichbar wirksame Kontrollmaßnahmen regelt der Entwurf ebenso wenig wie Verpflichtungen zur Dokumentation und Begründung der Nutzung der Analyseplattform. Nur durch Dokumentation und Kontrolle kann jedoch der eingeschränkte Individualrechtsschutz bei der ohne Wissen der Betroffenen erfolgenden Datenanalyse ausgeglichen werden.

e. Wesentlichkeitsgrundsatz, Gesetzesvorbehalt, Bestimmtheit und Normenklarheit im Übrigen

Auch im Übrigen genügt die Norm im vorliegenden Entwurf nicht dem verfassungsrechtlichen Gesetzesvorbehalt und Wesentlichkeitsgrundsatz. Für eine verfassungsrechtliche Rechtfertigung, gerade bei Eingriffsschwellen unterhalb der mindestens konkretisierten Gefahr ist erforderlich, dass Analyse- und Auswertungsmöglichkeiten durch den Gesetzgeber normenklar und hinreichend bestimmt begrenzt werden.[26] Der Gesetzgeber darf die Regelungsaufgabe zwar zum Teil der Verwaltung durch Verordnungsermächtigung überlassen, muss aber sicherstellen, dass ausreichende Regelungen zu Art und Umfang der Daten und zur Beschränkung der Datenverarbeitungsmethoden im Gesetz geregelt sind.[27] § 30a des Entwurfs genügt diesen Anforderungen nicht. Der Entwurf enthält insbesondere wie bereits ausgeführt **keine ausreichenden Begrenzungen von Art und Umfang der verwendeten Daten sowie** der **Analysemethoden.** Daneben fehlt es an zureichenden gesetzlichen Regelungen zu **Dokumentation und Veröffentlichung** der maßgeblichen Konkretisierung und Standardisierung seitens der Behörde.[28] Da die verwendeten Datenbestände nicht von vorherein inhaltlich und mengenmäßig sehr eng begrenzt sind, bedarf es zudem einer gesetzlichen Einschränkung des Zugriffs auf die Analyseeinrichtung auf einzelne, entsprechend qualifizierte Mitarbeitende.[29] Weiterhin fehlt es in § 30a des Entwurfs an **expliziten Vorkehrungen gegen eine unangemessen verzerrende und diskriminierende Wirkung der Datenauswahl**, gerade für den Einsatz von künstlicher Intelligenz.[30]

Dass der Entwurf in § 30a Abs. 8 eine Verordnungsermächtigung für das zuständige Ministerium zur Regelung von Art und Umfang der analysierten Daten, der technischen Ausprägung der eingesetzten Methoden, der Erteilung von Zugriffsberechtigungen, der Aufrechterhaltung bestehender Kennzeichnungen und weiteren technischen Vorkehrungen zur Sicherstellung der

---

26 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 110.
27 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 110.
28 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 113; BVerfG, Urteil vom 24. April 2013, 1 BvR 1215/07, Rn. 183.
29 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 117.
30 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 95, 100.

Zweckbindung sowie zu Protokollierung und Dokumentation der Datenanalysen enthält, genügt für eine Wahrung des Gesetzesvorbehalts nicht. Damit Einschränkungen das Eingriffsgewicht mildern, müssen diese im Wesentlichen im Gesetz selbst geregelt oder durch dieses vorgegeben und durch die Verwaltung klar abstrakt geregelt und veröffentlicht sein.[31] Der Entwurf sieht jedoch keine ausreichenden Vorgaben vor und überlässt damit grundrechtswesentliche Abwägungsentscheidungen dem Verordnungsgeber.

2. Strategische Datenanalyse

Für die strategische Datenanalyse ergibt sich in der vorliegenden Fassung des § 30a Abs. 2, 7 des Entwurfs kein anderes Ergebnis. Es handelt sich ebenso um einen **besonders schweren, jedenfalls nicht um einen nur geringfügigen Grundrechtseingriff.**

Hinsichtlich Art, Umfang und Herkunft der Daten sowie hinsichtlich der vorgesehenen Analysemethoden unterscheidet sich die strategische Datenanalyse nicht von der operativen und sieht damit eine Möglichkeit zur Analyse eines erheblichen, kaum übersehbaren Umfangs auch sehr grundrechtssensibler Daten mit weitgehenden und komplexen Analysemethoden vor. Sie unterscheidet sich damit erheblich von Maßnahmen, die auch ohne automatisierte Anwendungen, wenn auch aufwändiger und langsamer, erlangt werden könnten und geht wesentlich über einen einfachen Datenabgleich hinaus.[32]

Auch sind die Ziele bzw. Anlässe der strategischen Datenanalyse nicht ausreichend begrenzt, um das Eingriffsgewicht deutlich zu reduzieren. Dies ist schon deshalb der Fall, weil die Anlässe in § 30a Abs. 2 S. 2 des Entwurfs nicht abschließend geregelt sind („insbesondere"). Darüber hinaus kann die strategische Datenanalyse neben weniger eingriffsintensiven Analysezielen wie der Ermittlung gefährlicher oder gefährdeter Orte[33] auch explizit zu statistischen Zwecken und zur Ermittlung von Kriminalitätsphänomenen und Tätergruppierungen herangenzogen werden. Letztere weisen ein erhöhtes Eingriffsgewicht auf. Im Falle der Ermittlung von Tätergruppierungen stellt sich bereits die Frage, wie eine solche Ermittlung sinnvoll ohne personenbezogene Daten erfolgen soll. In diesen Bereichen besteht vielmehr die Gefahr, dass gerade besonders diskriminierungssensible personenbezogene Daten wie Geschlecht, Herkunft und Migrationsgeschichte sowie äußerliche Merkmale zur Analyse herangezogen werden. Darüber hinaus besteht bei dem Gebrauch komplexer Systeme zu statistischen Zwecken ein besonderes Risiko, da allein statistische Auffälligkeiten in einer Datenmenge entdeckt werden und zur Grundlage von unbegrenzten weiteren Analyseschritten mit offenem Analyseergebnis genommen

---

31 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 119.
32 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 108.
33 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 108.

werden können.[34] In jedem Falle bedürfte es für die Auswertung auch anonymer und pseudonymisierter Daten explizite Vorgaben zum Schutz vor diskriminierenden Algorithmen, Analyseschritten und -ergebnissen sowie zur Fehlererkennung und -vermeidung.

Zwar soll die strategische Datenanalyse nach § 30a Abs. 2, 7 des Entwurfs erkennbar vor allem mit anonymisierten und nur nachrangig mit pseudonymisierten personenbezogenen Daten betrieben werden. Die Verwendung personenbezogener Daten ist nur zulässig, soweit eine Weiterverarbeitung anonymisierter Daten zu diesem Zweck nicht möglich ist und das öffentliche Interesse an der strategischen Datenanalyse das schutzwürdige Interesse der Person erheblich überwiegt, § 30a Abs. 7 S. 2 des Entwurfs. Auch sind die Daten in diesem Falle gemäß § 30a Abs. 7 S. 3 des Entwurfs zu pseudonymisieren.

Jedoch stellt die **Pseudonymisierung** in diesem Falle vor dem Hintergrund der erheblichen Analysemöglichkeiten einen **nur unzureichenden Schutz** dar, da eine Identifikation der Dateninhaber*innen durch eine solche gerade nicht wirksam verhindert werden kann. Auch schließt der Entwurf nicht aus, dass eine Pseudonymisierung aus Anlass der Ergebnisse einer strategischen Datenanalyse rückgängig gemacht werden könnte.

Die nur unzureichende Beschränkung der Norm durch ihre nicht abschließend und zu weitgehend geregelten Analyseziele besteht ein **nicht unerhebliches Risiko**, dass die strategische Analyse **missbräuchlich zur Umgehung der Eingriffsschwellen der operativen Datenanalyse** auch im Einzelfall der polizeilichen Arbeit gebraucht werden könnte.

II. Keine verfassungsrechtliche Rechtfertigung der Eingriffe

Da es sich bei operativer und strategischer Datenanalyse um schwerwiegende, jedenfalls nicht nur geringfügige Grundrechtseingriffe handelt, genügen die geregelten Eingriffsvoraussetzungen, insbesondere die Eingriffsschwellen und die zu schützenden Rechtsgüter nicht zur verfassungsrechtlichen Rechtfertigung der Maßnahmen. Im Ergebnis stellt der vorliegende § 30a des Entwurfs sowohl hinsichtlich der operativen als auch der strategischen Datenanalyse eine verfassungswidrige Verletzung des Rechts auf informationelle Selbstbestimmung gemäß Art. 2 Abs. 1 i.V.m Art. 1 Abs. 1 GG dar. Weiterhin betrifft die Norm Art. 10 GG, da auch Daten aus Telekommunikationsüberwachung in die Analysen einbezogen werden dürfen, sowie das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG).

---

[34] BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 147.

1. Operative Datenanalyse

Zur Rechtfertigung der operativen Datenanalyse als schwerwiegender Grundrechtseingriff bedarf es einer Einschränkung des Einsatzes auf Fälle einer zumindest konkretisierten Gefahr für besonders gewichtiges Rechtsgut. Diesen Anforderungen genügen die in § 30a Abs. 6 S. 1 Nr. 1-3 des Entwurfs nicht. Insbesondere enthält § 30a Abs. 6 Nr. 3 des Entwurfs eine unzulässige dynamische Verweisung auf die bundesgesetzlichen §§ 100a f. StPO.

Die Eingriffsvoraussetzungen des § 30a Abs. 6 S. 1 Nr. 1 des Entwurfs fordern die Abwehr einer erheblichen Gefahr. Diese ist in § 3 Nr. 3 lit. c SOG LSA als „eine Gefahr für ein bedeutsames Rechtsgut, wie Leben, Gesundheit, Freiheit, wesentliche Vermögenswerte oder der Bestand des Staates" definiert. Diese Schwelle genügt weitestgehend den verfassungsrechtlichen Anforderungen. Allerdings ist ein schwerwiegender Grundrechtseingriff nicht zum Schutz aller wesentlichen Vermögenswerte zulässig, sondern nur zum Schutz von Sachen, deren Erhalt im öffentlichen Interesse geboten ist, z.B. bei wesentlichen Infrastruktureinrichtungen oder sonstigen Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen.[35] Insoweit genügt die Schwelle den verfassungsrechtlichen Anforderungen nur im Falle einer verfassungskonform engen Auslegung.

Anders ist § 30a Abs. 6 S. 1 Nr. 2 des Entwurfs zu beurteilen. Zunächst es bereits an einer ausreichenden Regelung einer zumindest konkretisierten Gefahr. Diese setzt voraus, dass bestimmte festgestellte Tatsachen die Prognose der Entstehung einer konkreten Gefahr tragen. Dies wiederum erfordert nicht nur, dass der Schluss auf ein der Art nach und zeitlich konkretisiertes Geschehen möglich ist, sondern auch, dass bestimmte Personen beteiligt sein werden, die so weit identifiziert werden können, dass Überwachungsmaßnahmen gezielt gegen sie gerichtet und auf sie weitestgehend beschränkt werden können.[36] Diesen Anforderungen an die Eingriffsschwelle genügt § 30a Abs. 6 S. 1 Nr. 2 des Entwurfs nicht, da er **keine personelle Konkretisierung der Gefahr** fordert. Dies kann auch nicht aus § 30a Abs. 4 S. 1 des Entwurfs und den dort genannten Personen hergeleitet werden, da dieser keine Regelungen hinsichtlich der Zielpersonen trifft und wie bereits dargestellt auch eine erhebliche Zahl von Personenkreisen umfasst, die für eine Maßnahmerichtung gerade keinen Anlass geboten haben.

Auch genügen die in Bezug genommenen Straftaten von erheblicher Bedeutung gemäß § 3 Nr. 4 SOG LSA nicht als **erforderliche besonders gewichtige Rechtgüter**. Dieser gesetzliche Katalog umfasst auch **einfache Vergehen,** beispielsweise besonders schwere Fälle des Diebstahls nach § 243 StGB und den einfachen Computerbetrug gemäß § 263a StGB. Ebenso sind Vorfeldstraftaten wie § 129 StGB erfasst, ohne dass die Norm eine zusätzliche konkretisierte Gefahr für Rechtsgüter fordert. Weiterhin enthält die Norm eine noch weitergehende Öffnungsklausel (§ 3 Nr. 4 S. 2 SOG

---

35 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 105 m.w.N.

36 BVerfG, Urteil vom 16. Februar 2023, 1 BvR 1547/19, 1 BvR 2634/20, Rn. 106 m.w.N.

LSA) für weitere, nicht genannte Delikte. Die genannten Straftaten genügen daher schon aus Bestimmtheitsgründen, aber auch mangels Schutzes überragend wichtiger Rechtsgüter nicht zur Rechtfertigung eines schwerwiegenden Grundrechtseingriffes.

Gleiches gilt für § 30a Abs. 6 S. 1 Nr. 3 des Entwurfs. Hier fehlt es bei der Eingriffsschwelle sowohl an dem **Erfordernis einer Konkretisierung in zeitlicher Sicht und der Art nach als auch in persönlicher Hinsicht**. Darüber hinaus genügt der Katalog des § 100a Abs. 2 StPO nicht zum Schutz überragend wichtiger Rechtsgüter, da er insbesondere auch einfache Vermögensdelikte (§ 100a Abs. 2 Nr. 1 lit. j, k, m StPO) genügen lässt.

Vor allem stellt aber der **Verweis auf die Straftatenkataloge der §§ 100a f. StPO eine unzulässige dynamische Verweisung** dar, mit welcher der Gesetzgeber Sachsen-Anhalts seine originäre Abwägung der zu schützenden Rechtsgüter nicht ausreichend wahrnimmt.[37] Ein dynamischer Verweis auf einen bundesgesetzlichen Katalog birgt das Risiko, dass Änderungen der StPO das Eingriffsgewicht des § 30a Abs. 6 S. 1 Nr. 3 des Entwurfs ohne Zutun des Landesgesetzgebers verändern können.

Selbst, wenn man in der operativen Datenanalyse nur einen weniger gewichtigen Eingriff ansehen und deswegen nur geringere Anlässe zur Rechtfertigung genügen ließe, genügten die geregelten Eingriffsschwellen und die zu schützenden Rechtsgüter nicht den verfassungsrechtlichen Anforderungen. Hierzu können entweder an die Eingriffsschwelle der zumindest konkretisierten Gefahr **oder** an die zu schützenden Rechtsgüter geringere Anforderungen gestellt werden, sodass der Schutz von Rechtsgütern von zumindest erheblichem Gewicht ausreicht.

Die Eingriffsvoraussetzungen der § 30a Abs. 6 S. 1 Nr. 2 und 3 des Entwurfs werden jedoch auch diesen Anforderungen nicht gerecht, da **sowohl** an die Eingriffsschwelle **als auch** an die zu schützenden Rechtsgüter geringere Anforderungen als erforderlich gestellt werden. Da beide Rechtsgrundlagen wie bereits dargestellt die Eingriffsschwelle einer konkretisierten Gefahr nicht voraussetzen, kann nicht zugleich auf den Schutz nur erheblicher Rechtsgüter abgestellt werden. Weiterhin ist auch in diesem Fall der dynamische Verweis auf die §§ 100a f. StPO verfassungsrechtlich unzulässig.

2. Strategische Datenanalyse

Da auch die strategische Datenanalyse in der mit dem Entwurf vorgelegten Ausgestaltung einen schwerwiegenden, jedenfalls einen nicht ganz geringfügigen Grundrechtseingriff darstellt, bedarf es auch für diese der Regelung zusätzlicher Eingriffsvoraussetzungen nach den bereits dargestellten Maßstäben.

---

37 BVerfG, Urteil vom 26. April 2022, 1 BvR 1619/17, Rn. 385.

Darüber hinaus und unabhängig vom Eingriffsgewicht sollten für die strategische Datenanalyse in § 30a Abs. 7 des Entwurfs die einfachgesetzlichen Zweckbindungsgrundsätze des § 13b SOG LSA in Bezug genommen werden. Darüber hinaus bedarf es gerade mit Blick auf die Nutzung zur Erstellung von Tätergruppierungen und zu statistischen Zwecken der gesetzlichen Regelung von Maßnahmen, um Fehler und vor allem diskriminierende Analyseabläufe und -ergebnisse zu erkennen und zu vermeiden.

III. Fehlende Gesetzeskompetenz

Soweit § 30a Abs. 1 des Entwurfs auf „polizeiliche Ermittlungen zur Strafverfolgung" Bezug nimmt, mangelt es dem Entwurf zudem an einer verfassungsrechtlichen Gesetzgebungskompetenz. Nach ständiger Rechtsprechung des Bundesverfassungsgerichts sind Maßnahmen der Strafverfolgung Gesetzgebungskompetenz des Bundes.[38] Zwar können sich Gefahrenabwehr und Strafverfolgung inhaltlich und in ihrer Wirkung häufig überschneiden und doppelfunktionale Maßnahmen zulässigerweise auch in Landesgesetzen zur Gefahrenabwehr verankert sein.[39] Maßgeblich ist dabei jedoch der objektivierte Zweck der Maßnahme.[40] Liegt der Schwerpunkt einer Maßnahme eindeutig auf der Strafverfolgung, so ist eine Ermächtigung durch die bundesgesetzliche Strafprozessordnung erforderlich.[41] Landesrechtliche Normen, die solche Maßnahmen ermöglichen, sind dagegen mit der Kompetenzregelung des Art. 74 Abs. 1 Nr. 1 GG unvereinbar. Insofern sollte der explizite Verweis auf die Anwendung zur „Strafverfolgung" in § 30a Abs. 1 des Entwurfs ersatzlos gestrichen werden.

C. Technologieoffenheit der Software

Über den konkreten Entwurf hinaus sollte bei Ausführung der im Entwurf vorgesehenen Datenanalysen nicht auf Software privater Anbieter*innen, sondern auf staatliche und unternehmensunabhängige Software zurückgegriffen werden. Zwar ist der Einsatz privater Software im Rahmen staatlicher Datenverarbeitung nicht per se ausgeschlossen.[42] Die Auslagerung des Grundrechts- und Datenschutzes vom grundrechtsverpflichteten Staat auf private Unternehmen ist im Bereich der Polizeiarbeit und der damit einhergehenden sensiblen und persönlichkeitsrechtsrelevanten Daten jedoch risikoreich. **Manipulation und mögliche Hintertüren** und damit das **Risiko von Datenleaks sensibler polizeilicher Daten** können **nie**

---

38 BVerfG, Beschluss vom 18. Dezember 2018, 1 BvR 142/15, Rn. 67; vgl. auch BVerfG, Urteil vom 15. Dezember 1970, 2 BvF 1/69, 2 BvR 629/68, 2 BvR 308/69, Rn. 108.

39 BVerfG, Beschluss vom 18. Dezember 2018, 1 BvR 142/15, Rn. 72 ff.; BVerfG, Beschluss vom 18. Dezember 2018, 1 BvR 2795/09, 1 BvR 3187/10, Rn. 58 f.

40 BVerfG, Beschluss vom 18. Dezember 2018, 1 BvR 142/15, Rn. 73 f.; BVerfG, Beschluss vom 18. Dezember 2018, 1 BvR 2795/09, 1 BvR 3187/10, Rn. 59.

41 So wohl auch die Auffassung des BMI, BT-Drs. 20/8390, S. 5.

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

vollständig ausgeschlossen werden. Bei Wartung und Fehlerkorrektur besteht ein Risiko, dass Private Zugriff auf Datensätze und Analyseergebnisse erhalten. Dies gilt insbesondere für außereuropäische Anbieter*innen, die mit anderen Regierungen und Geheimdiensten auch autoritärer Staaten zusammenarbeiten. Zudem besteht die Gefahr, dass Algorithmen und Ergebnisse **intransparent** verbleiben und so Fehler und insbesondere diskriminierende und verzerrende Algorithmen schlechter identifiziert und beseitigt werden können.

Auch ist die Kostenersparnis bei der Nutzung privater Softwareangebote kein aussagekräftiges Argument, da auch die Lizensierung einer privaten Software mit erheblichen Kosten verbunden ist.[43] Dies gilt umso mehr, wenn Anbieter*innen bei deutschen Behörden eine weitgehende Monopolstellung einnehmen und so die Abhängigkeit von der angebotenen Software zur Preisgestaltung ausnutzen können.

Für den Betrieb der geregelten Analysevarianten sollte das Land Sachsen-Anhalt daher auf eine bund- und länderübergreifende staatliche Softwarelösung hinwirken.

---

[43] So entstanden beispielsweise in Nordrhein-Westfalen für eine auf Palantir Gotham beruhende Software statt ursprünglich geplanten 14 Millionen Euro nun Kosten iHv. 29 Millionen Euro, *Hell/Kartheuser*, NRW-Polizei: Knapp 40 Millionen Euro für umstrittene Palantir-Software, WDR vom 25. September 2022, abrufbar unter https://www1.wdr.de/nachrichten/landespolitik/nrw-polizei-datenbank-software-palantir-kosten-100.html#:~:text=Mittlerweile%20kostet%20das%20Gesamtprojekt%20das%20Land%20NRW%20insgesamt%2039%20Millionen%20Euro (zuletzt abgerufen am 6. Mai 2025).