Prof. Dr. iur. Kristin Pfeffer

FORSCHUNGSSTELLE EUROPÄISCHES UND DEUTSCHES SICHERHEITSRECHT (FEDS)

Prof. Dr. iur. Kristin Pfeffer, Hochschule der Polizei Hamburg, Überseering 35, 22297 Hamburg

An den Vorsitzenden des
Innen- und Rechtsausschusses
Jan Kürschner
Schleswig-Holsteinischer Landtag
Landeshaus,
Düsternbrooker Weg 70
24105 Kiel

Hochschule der Polizei Hamburg
University of Applied Sciences
Überseering 35
D-22297 Hamburg

E-Mail: kristin.pfeffer@ak.polizei.hamburg.de

Vorab per Email

Schleswig-Holsteinischer Landtag
Umdruck 20/6131

Entwurf eines Gesetzes zur Stärkung des Verfassungsschutzes im Lande Schleswig-Holstein

Gesetzentwurf der Landesregierung – Drucksache 20/3754

Hamburg, 17. Februar 2026

Sehr geehrte Damen und Herren Abgeordnete,

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

Mit freundlichen Grüßen

gez.

Kristin Pfeffer

Prof. Dr. iur. Kristin Pfeffer

FORSCHUNGSSTELLE EUROPÄISCHES UND DEUTSCHES SICHERHEITSRECHT (FEDS)

Stellungnahme

Zum Entwurf eines Gesetzes zur Stärkung des Verfassungsschutzes im Lande Schleswig-Holstein Gesetzentwurf der Landesregierung – Drucksache 20/3754

I. Vorbemerkung

Mit ihrem Gesetzesentwurf zur Stärkung des Verfassungsschutzes im Lande Schleswig-Holstein Gesetzentwurf der Landesregierung schlägt die Landesregierung neue Eingriffsbefugnisse für den Verfassungsschutz vor, die erkennbar von dem Anspruch geprägt sind,

- die Effektivität der Arbeit des Verfassungsschutzes zu erhöhen,
- insbesondere auf die rasante Fortentwicklung der Datafizierung der Arbeit der Nachrichtendienste zu reagieren,
- die zwischenzeitlich ergangen Entscheidungen des BVerfG von 2023 umzusetzen.

Die nachfolgende Stellungnahme beschränkt sich auf einige Anmerkungen zu dem Regelungsvorschlag in § 69 LVerfSchG-E (IT-gestützte Informationsanalyse).

Diese betreffende Befugnis ist äußerst eingriffsintensiv. Soweit auf Nachrichtendienste anwendbar, sind hier Vorgaben des BVerfG (Urteil vom 16. Februar 2023 - 1 BvR 1547/19 zu den Eingriffsbefugnissen von Hamburg und Hessen) zu beachten. Vor einer Verabschiedung empfehle ich den Vorschlag noch in einigen Punkten anzupassen.

II. Prüfungsmaßstab

Im mitgliedstaatlichen Sicherheitsrecht folgen Vorgaben für die automatisierte Datenanalyse im Bereich Gefahrenabwehr und Strafverfolgung inzwischen auch aus der Verordnung zur Harmonisierung der mitgliedstaatlichen Gesetze im Bereich des Einsatzes künstlicher Intelligenz, der VO (EU) 2024/1689 (KI-VO).[1] Die KI-VO verfolgt (erstmalig) einen sektorenübergreifenden Regelungsansatz, der die charakteristischen Herausforderungen der Regulierung von und des Umgangs mit KI-Systemen in Angriff nimmt und deren gesamten “Lebenszyklus” (von der Entwicklung bis zur Verwendung) erfasst. Auch Sicherheitsbehörden unterliegen damit nun künftig den Anforderungen der KI-VO.[2] Die EU stützt sich hierbei auf ihre Kompetenz aus Art. 114 AEUV zur Binnenmarktregulierung und Art. 16 AEUV zum Datenschutz, ErwGr 3. Ziel des Gesetzes ist ein funktionierender Binnenmarkt durch einen einheitlichen Rechtsrahmen, insbesondere für die Entwicklung, das Inverkehrbringen, die Inbetriebnahme und die Verwendung von Systemen künstlicher Intelligenz (KI-Systeme) in der Union unter

[1] Pfeffer, NVwZ 2022, S. 294 ff.; zum Harmonisierungsgrad des Polizeirechts durch die KI-VO Hofmann-Coombe, EuR 2025, S. 363, 376 ff.

[2] Dazu eingehend Pfeffer, Der Einsatz künstlicher Intelligenz in der Polizeiarbeit nach dem AI-Act – Eine rechtswissenschaftliche Perspektive, in: Honekamp, Wilfried/Kemme, Stefanie (Hrsg.), Auswirkungen von KI auf die zukünftige Polizeiarbeit 2025, S. 31ff.

Beachtung der Werte der Union, Förderung der Technologie unter gleichzeitiger Beachtung der Grundrechte, Art. 1 Abs. 1 KI-VO.

Die Arbeit des mitgliedstaatlichen Verfassungsschutzes unterliegt – anders als das übrigen Sicherheitsrecht – jedoch keiner Europäisierung/Harmonisierung. Nach dem Europäischen Primärrecht verbleibt die alleinige Verantwortung für die nationale Sicherheit und Aufrechterhaltung der öffentlichen Ordnung bei den Mitgliedstaaten, Art. 4 Abs. 2 Satz 3 EUV (sog. ordre-public-Vorbehalt). Der EuGH legt den Begriff der „nationalen Sicherheit" in ständiger Rechtsprechung eng aus. Es gehe dabei um den Schutz der wesentlichen Funktionen des Staates und der grundlegenden Interessen der Gesellschaft, um „die Verhütung und Repression von Tätigkeiten, die geeignet sind, die tragenden Strukturen eines Landes im Bereich der Verfassung, Politik oder Wirtschaft oder im sozialen Bereich in schwerwiegender Weise zu destabilisieren und insbesondere die Gesellschaft, die Bevölkerung oder den Staat als solchen unmittelbar zu bedrohen (…)". Letzteres umfasse insbesondere die Verhütung und Repression von terroristischen Aktivitäten.[3] Die Bekämpfung schwerer Kriminalität wird vom EuGH dagegen (nur) unter den Begriff „innere Sicherheit" subsumiert.[4]

§ 69 LVerfSchG-E erlaubt eine IT-gestützte Informationsanalyse im Bereich der Aufgaben des Landesverfassungsschutzes gem. §§ 8-14 LVerfSchG-E. Eingriffstatbestände zu den hier genannten Aufgaben betreffen die nationale Sicherheit iSd Art. 4 Abs. 2 Satz 2 EUV iVm Art. 2 Abs. 3 UAbs. 1 KI-VO.

KI-Systeme, die für die „nationale Sicherheit" eingesetzt werden, fallen nicht in den Anwendungsbereich der KI-VO (Art. 2 Abs. 3 UAbs. 1 KI-VO iVm Art. 4 Abs. 2 Satz 3 EUV).

Der Prüfungsmaßstab bleibt hier das Grundgesetz.

III. Grundgesetzlicher Rahmen

1. Befugnisbezogenes Trennungsgebot zwischen Nachrichtendiensten und Polizei

Die Verankerung der IT-gestützten Informationsanalyse in § 69 LVerfSchG-E für den Landesverfassungsschutz dürfte nicht gegen das verfassungsrechtliche Trennungsverbot zwischen Nachrichtendiensten und Polizei verstoßen. Die jüngste Rechtsprechung des BVerfG defininert das Trennungsgebot zwischen Nachrichtendiensten und Polizei befugnisbezogen.[5] Danach darf der Verfassungsschutz als Nachrichtendienst selbst nicht mit operativen Eingriffsbefugnissen ausgestattet werden. Denn das verfassungsrechtliche Privileg für nachrichtendienstliche Überwachungen ist nur dann gerechtfertigt, wenn gewährleistet ist, dass die weitreichenden Überwachungsbefugnisse der Nachrichtendienste und die weitreichenden operativen Befugnisse anderer Sicherheitsbehörden grundsätzlich voneinander getrennt bleiben. Demzufolge dürfen Nachrichtendienste weder zu ständigen

[3] EuGH 21.6.2022 – C-817/19 – Ligues des droits humaines.

[4] EuGH 5.4.2022 – C-140/20 – Commissioner of An Garda Síochána. Zum Trennungsprinzip zwischen Polizei und Geheimdiensten Denninger, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, B. Rn. 43ff.; Zur grundsätzlichen Aufgabentrennung von Polizei und Militär Weingärtner, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, I. Rn. 679ff; Zu den Konflikten bei der Auslegung des Begriffs nationale Sicherheit Pfeffer, NVwZ 2023, S. 1288.

[5] Bäcker, in: Lisken/Denninger, Handbuch des Polizeirechts, 8. Auflage 2026, Kapitel 2, Rn. 358, 362.

Informationshelfern der operativ tätigen Sicherheitsbehörden werden, noch dürfen sie sich dieser Behörden bedienen, um ihren Befugniskreis um imperative Eingriffe zu erweitern.[6]

Die nachrichtendiensttypischen Befugnisse zur Sammlung und Analyse von Informationen sind nicht als operative Befugnisse einzustufen.[7] Die hier betrachtete IT-gestütze Informationsanalyse in § 69 LVerfSchG-E ist auch der nachrichtendiensttypischen Informationsanalayse zuzurechnen. Der Verankerung in § 69 LVerfSchG-E verstößt daher nicht gegen das verfassungsrechtliche Trennungsgebot zwischen Nachrichtendiensten und Polizei.

2. Rechtsprechung des BVerfG vom 16. Februar 2023

Mit Urteil vom 16. Februar 2023 hat das BVerfG die Ermächtigungsgrundlagen zur automatisierten Datenanalyse im Hessischen Polizeigesetz (§ 25a HSOG a.F.) sowie im Hamburgischen Gesetz über die Datenverarbeitung der Polizei (§ 49 HmbPolDVG a.F.) für verfassungswidrig erklärt. Nach Auffassung des Gerichts verstoßen die Regelungen gegen das allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG in seiner Ausprägung als Recht auf informationelle Selbstbestimmung.[8]

Das Gericht stellt dabei zunächst klar, dass der Gesetzesvorbehalt nicht nur die erstmalige Erhebung personenbezogener Daten erfasst, sondern ebenso deren weitere Verarbeitung und Zweckänderung.[9] Die automatisierte Analyse bereits rechtmäßig erhobener Daten stellt danach einen eigenständigen Grundrechtseingriff dar, der nicht durch die ursprüngliche Erhebungsbefugnis legitimiert wird, sondern einer eigenen, hinreichend bestimmten gesetzlichen Ermächtigungsgrundlage bedarf.[10] Maßgeblich ist, dass durch die algorithmische Verknüpfung und Auswertung vorhandener Daten neues Wissen generiert wird, das Rückschlüsse auf betroffene Personen ermöglicht und qualitativ über den ursprünglichen Erhebungszusammenhang hinausgeht.[11]
Das BVerfG bejaht den legitimen Zweck der automatisierten Datenanalyse ebenso wie deren grundsätzliche Geeignetheit und Erforderlichkeit zur vorbeugenden Bekämpfung schwerer Straftaten.[12]

Verfassungsrechtlich entscheidend ist jedoch die Verhältnismäßigkeit im engeren Sinne. Diese hängt maßgeblich vom Gewicht des Grundrechtseingriffs ab, welches das Gericht bei der automatisierten Datenanalyse als besonders hoch einstuft.[13] Die besosndere Eingriffsintensität ergibt sich nach Auffassung des Gerichts aus den der Maßnahme immanenten Belastungseffekten,[14] die unabhängig vom Gewicht der ursprünglichen Datenerhebung bestehen. Die automatisierte Zusammenführung umfangreicher und

[6] Bäcker, in: Lisken/Denninger, Handbuch des Polizeirechts, 8. Auflage 2026, Kapitel 2, Rn. 358, 360.
[7] Bäcker, in: Lisken/Denninger, Handbuch des Polizeirechts, 8. Auflage 2026, Kapitel 2, Rn. 358, 360.
[8] BVerfG - 1 BvR 1547/19; 1 BvR 2634/20 Rn. 152 ff., Nr. 2 des Tenors.
[9] BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 61.
[10] BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20, Rn. 55; Weisser GSZ 2023, 183 (185).
[11] BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 142.
[12] BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 52, 53.
[13] BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 59, 64.
[14] BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 66, 67.

heterogener Datenbestände verleiht der Maßnahme ein eigenständiges „Eigengewicht“.[15] Dieses resultiert insbesondere aus der gesteigerten Effektivität polizeilicher Informationsverarbeitung, die es erlaubt, in kurzer Zeit komplexe Beziehungsgeflechte, Muster und Zusammenhänge zu erkennen oder überhaupt erst herzustellen.[16] Damit wirkt die automatisierte Datenanalyse regelmäßig vorgelagert zu weiteren polizeilichen Maßnahmen und beeinflusst die präventive Gefahrenprognose, von der wiederum die Reichweite nachfolgender Eingriffsbefugnisse abhängt.

Über dieses vom BVerfG hervorgehobene Eigengewicht hinaus ist jedoch zu berücksichtigen, dass die automatisierte Datenanalyse nicht lediglich einen einzelnen informationellen Grundrechtseingriff intensiviert, sondern strukturell auf die gesamte Architektur polizeilicher Eingriffsbefugnisse zurückwirkt.[17] Sie setzt nicht erst auf der Ebene konkreter Eingriffsmaßnahmen an, sondern betrifft die vorgelagerte Stufe der polizeilichen Gefahrenprognose selbst und verändert damit die tatsächliche Grundlage, von der aus über das Vorliegen gesetzlicher Gefahrenschwellen entschieden wird. Während klassische Gefahrenprognosen typischerweise auf einer begrenzten, durch menschliche Wahrnehmungs- und Kombinationsfähigkeiten geprägten Tatsachengrundlage beruhen, ermöglichen automatisierte Analyseverfahren die nahezu augenblickliche Verdichtung vorhandener Datenbestände sowie die Erzeugung neuer, komplexer Beziehungs- und Verdachtslagen. Dadurch verschiebt sich das faktische Gewicht der Gefahreneinschätzung, ohne dass der Gesetzgeber die formellen Eingriffsschwellen selbst angepasst hätte. Die Maßnahme wirkt insoweit entgrenzend, indem sie bestehende Schwellenwerte nicht normativ absenkt, sondern technologisch unterläuft. In dieser Perspektive ist die automatisierte Datenanalyse nicht nur als eigenständiger Grundrechtseingriff, sondern als strukturprägendes Instrument der polizeilichen Gefahrenabwehr zu begreifen.

Vor diesem Hintergrund betont das BVerfG, dass bestehende Eingriffsschwellen vielfach unter der Prämisse begrenzter menschlicher Auswertungs- und Kombinationsfähigkeiten entwickelt worden seien. Diese Annahme verliere angesichts moderner Analyseverfahren an Tragfähigkeit. In einer zunehmend datafizierten Gesellschaft bestehe daher die Gefahr einer strukturellen Ausweitung polizeilicher Eingriffsmöglichkeiten, sofern der Gesetzgeber dem nicht durch klare normative Begrenzungen entgegenwirkt.

Die angegriffenen Ermächtigungsgrundlagen aus Hamburg und Hessen genügten diesen Anforderungen nicht. Sie erlaubten eine daten- und methodenoffene Analyse polizeilicher Datenbestände, ohne Art, Umfang und Herkunft der einbezogenen Daten hinreichend zu bestimmen. Auch die tatbestandlichen Voraussetzungen der Maßnahme blieben zu unbestimmt.[18] Insbesondere genügten Formulierungen, die an einen „begründeten Einzelfall“ oder allgemein an die „vorbeugende Bekämpfung“ bestimmter Straftaten anknüpfen, nicht den verfassungsrechtlichen Anforderungen an eine tragfähige

[15] BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 67 ff. Ls. 3.
[16] BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 39.
[17] S. auch Lenschow, Eyk: Allwissende Polizei?: Entgrenzungen im Polizeirecht durch intelligente Gefahrenermittlung am Beispiel des SächsPVDG-E, VerfBlog, 2026/1/07, https://verfassungsblog.de/polizeigesetz-sachsen-referentenent-wurf/, DOI: 10.59704/dc1ccec73bb2e95b (Abruf: 16.01.2026)
[18] BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 131, 165.

Eingriffsschwelle. Nach Auffassung des Gerichts muss die automatisierte Datenanalyse jedenfalls auf die Identifizierung einer zumindest konkretisierten Gefahr für besonders gewichtige Rechtsgüter gerichtet sein und auf solche Daten beschränkt werden, die zur Abwehr dieser Gefahr geeignet sind.[19]

Die vom BVerfG betonte notwendige Eingriffsschwelle einer hinreichend konkretisierten Gefahr bei der polizeilichen automatisierten Datenanalyse lässt sich nicht auf nachrichtendienstlichen Maßnahmen übertragen (dazu unter V.).[20] Das Erfordernis einer polizeilichen Gefahr würde als generelle Eingriffsschwelle dem Aufgabenprofil einer Verfassungsschutzbehörde nicht gerecht.[21]

Auch im vorliegenden Fall bedeutsam ist es, dass der Gesetzgeber das Eingriffsgewicht der automatisierten Datenanalyse durch verschiedene normative Stellgrößen steuern kann:

Die Anforderungen an die Ermächtigungsgrundlagen zur automatisierten Datenanalyse sind danach abhängig von Art und Umfang der verarbeitbaren Daten und der zugelassenen Methode der Datenanalyse oder -auswertung.[22] Der Gesetzgeber kann die Eingriffsintensität in den Ermächtigungsgrundlagen danach zum einen über Tatbestandsvoraussetzungen steuern: Schwerwiegende Eingriffe in die informationelle Selbstbestimmung sind nur zum Schutz besonders gewichtiger Rechtsgüter möglich und sofern für diese eine zumindest hinreichend konkretisierte Gefahr besteht.[23] Eine Ausnahme besteht, 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 sind, weil dadurch das Eingriffsgewicht der Maßnahmen erheblich gemindert ist.[24] Der Gesetzgeber kann schließlich durch Verfahrensanforderungen für Nachvollziehbarkeit, Transparenz und behördliche Kontrolle sorgen, wie etwa mit Pflichten zur Kennzeichnung, Protokollierung oder Benachrichtigung.[25] Dabei gilt, je mehr Daten einbezogen werden (sensible Daten), desto weniger Zugriffsberechtigte sind zulässig. Hier sind Zugriffsbeschränkungen auf einen ausgewählten Kreis mit besonderer Qualifikation erforderlich.[26] Eine behördliche Kontrolle kann aber bei der automatisierten Datenanalyse wegen der hohen Anzahl von Verfahren nur über Stichproben durch Datenschutzbeauftragte erfolgen.[27]

Das BVerfG hat mithin zahlreiche Faktoren aufgezeigt, über die das Eingriffsgewicht in die informationelle Selbstbestimmung durch den Gesetzgeber gesteuert werden kann, dem die Aufgabe obliegt, in der gesetzlichen Regelung ein angemessenes Verhältnis zwischen der Eingriffsschwelle und der bezweckten Gefahrenabwehr zu finden.[28]

[19] BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 164 ff.
[20] BVerfG, Urteil v. 26. April 2022 - 1 BvR 1619/17 -, Rn. 161 ff.
[21] BVerfG, Urteil v. 26. April 2022 - 1 BvR 1619/17 -, Rn. 163.
[22] Dazu eingehend Kugelmann/Buchmann, GSZ 2024, S. 1ff.
[23] BVerfG, Urteil v. 1.10.2024 - 1 BvR 1160/19 Rn. 103 ff.
[24] Kugelmann/Buchmann, GSZ 2024, S. 1, 8 f.
[25] BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 109; Kugelmann/Buchmann, GSZ 2024, S. 1, 9f.
[26] Kugelmann/Buchmann, GSZ 2024, S. 1, 9.
[27] BVerfG, Urteil vom 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 109; Kugelmann/Buchmann, GSZ 2024, S. 1, 9.
[28] BVerfG, Urteil vom 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 103.

Außerdem kann der Gesetzgeber laut BVerfG die entsprechende Regelungsaufgabe auch zum Teil auf die Exekutive übertragen, wobei er die wesentlichen Grundlagen zur Begrenzung der Verarbeitungsmethoden und von Art und Umfang der Daten selbst zu regeln hat, um dem Gesetzesvorbehalt zu entsprechen.[29]

Automatisierte Datenanalysen im Sicherheitsrecht sind danach nicht von vornherein ausgeschlossen, setzen jedoch eine präzise gesetzgeberische Entscheidung über Eingriffsschwelle, Datenumfang und Zweckbindung voraus. Die vom Bundesverfassungsgericht entwickelten Maßstäbe zwingen den Gesetzgeber damit zu einer Neubewertung bestehender Ermächtigungsgrundlagen, in der die gesteigerte Leistungsfähigkeit algorithmischer Analyseinstrumente normativ reflektiert und durch hinreichend bestimmte Regelungen in ein angemessenes Verhältnis zum Grundrecht auf informationelle Selbstbestimmung gesetzt wird.

3. Einbeziehung privater Dienstleister

Unter Berufung auf die verfassungsrechtlich gebotene digitale Souveränität weisen zahlreiche Kritiker derzeit darauf hin, dass bei der Einbeziehung privater Dienstleister im Bereich von eingriffsintensiven Maßnahmen größte Zurückhaltung geboten ist.[30] Die Konferenz der unabhängigen deutschen Datenschutzaufsichtsbehörden der Länder und des Bundes betonte im September 2025 im Hinblick auf den Einsatz von Software zur automatisierten Datenanalyse ausdrücklich, dass bei sicherheitsbehördlichen Datenbeständen eine Schutzpflicht gegenüber den Grundrechtsträgern besteht, dass Daten nicht ohne vorherige Prüfung in Drittstaaten weiterverwendet werden können, die hinter dem europäischen Rechtsstaatsniveau zurückbleiben. Darüber hinaus verlange die digitale Souveränität die Nachvollziehbarkeit und die Beherrschbarkeit der Datenverarbeitung, auch im Wege außergerichtlicher oder gerichtlicher Rechtsdurchsetzung, und die langfristige Vorhersehbarkeit und Verlässlichkeit des Angebots. Dies sei regelmäßig nur durch den Einsatz von Systemen erreichbar, deren Anbieter ihren Sitz im Europäischen Wirtschaftsraum (EWR) haben. Zur Wahrung der digitalen Souveränität durch Unterbindung von Abhängigkeiten sei sicherzustellen, dass die eingesetzten Systeme hinreichend offen sind, um nötigenfalls einen Wechsel auf ein geeigneteres System zu ermöglichen.[31]

IV. Automatisierte Datenanalyse durch Europol als „Service für die Sicherheitsbehörden der Mitgliedstaaten“

Im vorliegenden Zusammenhang ist auf Art. 18a VO (EU) 2022/991 hinzuweisen, wonach nationale Sicherheitsbehörde nunmehr Europol mit der Auswertung von Daten beauftragen können, sofern diese auch unter dem entsprechenden nationalen Rechtsrahmen in Ermittlungsverfahren ausgewertet und erhoben werden dürfen. Damit soll klargestellt

[29] BVerfG, Urteil vom 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 110, 112.
[30] Zum Ganzen Kelber/Bortnikov NJW 2023, S. 2000 ff.; Bäuerle, ZD 2025, S. 128, 131.
[31] Die Konferenz der unabhängigen der unabhängigen deutschen Datenschutzaufsichtsbehörden der Länder und des Bundes, Pressemitteilung v. 18.9.2025 zur verfassungskonformen Ausgestaltung automatisierter Datenanalysen durch Polizeibehörden.

werden, dass die Datenverarbeitung und Datenübermittlung möglich sind, solange sie den rechtlichen Anforderungen im jeweiligen Mitgliedsstaat genügen („Rechtmäßigkeitsfilter“).

Die automatisierte Datenanalyse wird vermehrt auch von den Europäischen Sicherheitsagenturen, wie etwa Europol eingesetzt.[32] Der Austausch und die Analyse von kriminalpolizeilichen Informationen gehört zu den Kernaufgaben Europols gem. Art. 88 Abs. 2, lit. a) AEUV. Europol hatte die Analyse-Software der Fa. Palantir Technologies Inc. zur automatisierten Datenanalyse eingesetzt,[33] bevor die VO (EU) 2022/991 einen Rechtsrahmen für die Verarbeitung und automatisierte Datenanalyse schuf: Danach sollen Bezüge zu anderen Kriminalitätsbereichen oder zu Ermittlungen in anderen Mitgliedstaaten hergestellt werden (Art. 18 Abs. 6a). Mit der Regelung soll klargestellt werden, dass die Agentur eingehende Daten vorab analysieren und feststellen kann, ob diese unter eine der zulässigen Kategorien des (Art. 18) fallen. Die betreffenden Daten sollen dann auch mit bereits vorliegenden abgeglichen werden dürfen. Europol soll so grenzüberschreitende Querverbindungen erfassen, welche die nationalen Behörden so nicht selbst hätten feststellen können. Insgesamt wird nun ausdrücklich die Befugnis zur automatisierten Datenanalyse als Service für die Mitgliedstaaten[34] und andere EU-Agenturen geregelt: Europol soll danach nicht nur Daten über verurteilte Straftäter und Tatverdächtige verarbeiten dürfen, sondern auch über *„Personen, in deren Fall nach Maßgabe des nationalen Rechts des betreffenden Mitgliedstaats faktische Anhaltspunkte oder triftige Gründe dafür vorliegen, dass sie Straftaten begehen werden, für die Europol zuständig ist.“*

Am 18. Dezember 2025 hat der Bundestag die Änderung des Europol-Gesetzes beschlossen, um dieses an die geänderte VO (EU) 2022/991 anzupassen.[35] Der darin neu eingefügte Absatz 1a Satz 1 in § 3 des Europol-Gesetzes erweitert künftig innerstaatlich die Möglichkeit der Übermittlung von Informationen durch die zuständigen nationalen Behörden über das Bundeskriminalamt auf den neuen Artikel 18a der Europol-Verordnung. Allerdings kann das neue Europol-Gesetz ausdrücklich nicht die materiellen und formellen Voraussetzungen und Bedingungen regeln, unter denen das Bundeskriminalamt, die Behörden der Bundespolizei und des Zolls, die weiteren Ermittlungsbehörden der Bundesfinanzverwaltung, die Polizeien der Länder sowie die mit der Steuerfahndung betrauten Dienststellen der Landesfinanzbehörden personenbezogene Daten an Europol übermitteln dürfen. Soweit

[32] Dazu Pfeffer, Die EU-Regulierung des KI-Einsatzes durch Sicherheitsbehörden - Zwischen nationaler Souveränität und Supranationalität, in: dies. (Hrsg.), AI and Policing in the Security Union – Chancen, Risiken und rechtliche Herausforderungen, Schriftenreihe der Forschungsstelle Europäisches und Deutsches Sicherheitsrecht (FEDS), Band 8, erscheint Anfang 2026.

[33] Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion DIE LINKE. – BT-Drs. 18/13194, Techniken zur Internetermittlung bei der Polizeiagentur Europol, BT-Drs. 18/13310, Antwort auf Frage 8; Vgl. ebenso: Antwort des Parlamentarischen Staatssekretärs Peter Tauber vom 26.04.2018 auf Anfrage des Abgeordneten Omid Nouripour (BÜNDNIS 90/DIE GRÜNEN), Frage 77 der Schriftlichen Fragen mit den in der Woche vom 30.04.2018 eingegangenen Antworten der Bundesregierung, BT-Drs. 19/1979.

[34] Die Bundesregierung hat den Entwurf eines Zweiten Gesetzes zur Änderung des Europol-Gesetzes vorgelegt, BT-Drs. 21/2373, v. 22.10.2025, welches innerstaatlich die Zuständigkeiten der beteiligten Behörden von Bund und Ländern bezüglich der Zusammenarbeit mit Europol sowie die Beziehungen dieser Behörden im Verhältnis zueinander bei der Zusammenarbeit mit Europol regeln soll.

[35] Gesetzentwurf der Bundesregierung Entwurf eines Zweiten Gesetzes zur Änderung des Europol-Gesetzes Drs. BT 21/2373 vom 22.10.2025.

diese Behörden Europol mit der automatisierten Datenanalyse beauftragten sollen, ist dafür zuvor eine Ermächtigungsgrundlage in den jeweiligen Fachgesetzen erforderlich.

Festzuhalten bleibt, dass mit der Schaffung der Ermächtigungsgrundlage für die automatisierte Datenanalyse in § 69 a NSOG-E künftig auch Europol mit einer automatisierten Datenanalyse beauftragt werden kann.

Dass eine Ermächtigungsgrundlage einer Sicherheitsbehörde eines Mitgliedstaates zur automatisierten Datenanalyse geeignet ist, die Art und Weise der Durchführung einer automatisierten Datenanalyse durch eine europäischen Agentur, die die automatisierte Datenanalyse „als Service“ für eine mitgliedstaatliche Sicherheitsbehörde durchführt, einzuhegen, erscheint mangels Bindungswirkung im Verhältnis zu EU-Agenturen fraglich.

V. Anmerkungen zur konkreten Ausgestaltung von § 69 LVerfSchG-E

Ein legitimer Zweck der It-gestützen Informationsanalyse ist ebenso zu bejahen, wie deren grundsätzliche Geeignetheit und Erforderlichkeit (dazu bereits unter IV.1,)[36]

Verfassungsrechtlich entscheidend ist jedoch die Verhältnismäßigkeit im engeren Sinne. Diese hängt maßgeblich vom Gewicht des Grundrechtseingriffs ab, welches das Gericht bei der automatisierten Datenanalyse als besonders hoch einstuft. Die Informationsauswertung mittels technischer Systeme, welche einen schwerwiegenden Eingriff in das Recht auf informationelle Selbstbestimmung ermöglicht, ist nur zum Schutz besonders gewichtiger Rechtsgüter zuzulassen.[37]

Der Schutz besonders gewichtiger Rechtsgüter ergibt sich vorliegend bereits aus den Aufgaben des Landesverfassungsschutzes gem. § 5 LVerfSchG-E iVm §§ 14-18 LVerfSchG-E.

Die Eingriffsschwelle einer hinreichend konkretisierten Gefahr bei der polizeilichen automatisierten Datenanalyse lässt sich nicht auf nachrichtendienstlichen Maßnahmen übertragen.[38] Das Erfordernis einer polizeilichen Gefahr würde als generelle Eingriffsschwelle dem Aufgabenprofil einer Verfassungsschutzbehörde nicht gerecht.[39]

Der Gesetzgeber kann das Eingriffsgewicht der automatisierten Datenanalyse durch verschiedene normative Stellgrößen steuern (dazu bereits unter IV.1.).

1. Art und Umfang der Daten

Der Umfang der einbeziehbaren Daten grundsätzlich sehr weit und nur an wenigen Stellen beschränkt:

Nach § 69 Abs. 1 LVerfSchG-E darf die Verfassungsschutzbehörde „zur Aufklärung von Bestrebungen oder Tätigkeiten nach §§ 8 bis 14 bereits erhobene Informationen, insbesondere im elektronischen Aktensystem oder im nachrichtendienstlichen Informationssystem

[36] BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 52, 53.
[37] BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 59, 64, 105, 107
[38] BVerfG, Urteil v. 26.04. 2022 - 1 BvR 1619/17 -, Rn. 161 ff.
[39] BVerfG, Urteil v. 26.04. 2022 - 1 BvR 1619/17 -, Rn. 163.

gespeicherte personenbezogene Informationen, auch unter Verwendung automatisierter technischer Systeme zur Informationsverarbeitung zusammenführen und anschließend zur Gewinnung neuer Erkenntnisse weiterverarbeiten (IT-gestützte Informationsanalyse).“

§ 69 Abs. 4 Satz 1 und 2 LVerfSchG-E schränkt den Umfang der einbeziehbaren Daten etwas ein ein: „In eine Informationsverarbeitung nach Absatz 1 dürfen solche Informationen einbezogen werden, die durch offene Erkenntnisse oder durch nachrichtendienstliche Mittel ohne besondere Eingriffsintensität gewonnen wurden. Informationen, die mit besonders eingriffsintensiven nachrichtendienstlichen Mitteln erhoben wurden, dürfen nur dann mit in die Analyse aufgenommen werden, wenn sie der Aufklärung besonders beobachtungsbedürftiger Bestrebungen gemäß § 34 Absatz 2 dienen.“ Der unbestimmte Begriff „ohne besondere Eingriffsintensität“ dürfte jedoch wenig geeignet sein, bestimmbar und klar abzugrenzen, welche Informationen aus welchen Maßnahmen einbezogen werden dürfen. Die Regelung trägt daher wenig dazu bei, die Eingriffstiefe der Maßnahme abzumildern.

Die Verarbeitung von Daten, die durch besonders schwere Grundrechtseingriffe erlangt wurden, wird durch § 69 Abs. 1 Satz 3, 4, 5 LVerfSchG-E nicht ausgeschlossen, aber begrenzt. Die Einbeziehung von Daten, die mit Hilfe von besonders schweren Grundrechtseingriffen erhoben worden sind, wird an enge Voraussetzungen knüpft: „Informationen, die aus Maßnahmen nach dem Artikel 10-Gesetz oder Wohnraumüberwachungen gewonnen wurden oder die einer besonderen Zweckbindung unterliegen, dürfen nur dann miteinbezogen werden, wenn auch für ihre Weiterverarbeitung die Voraussetzungen für diese Maßnahmen vorliegen. Bei Informationen aus Maßnahmen nach dem Artikel 10-Gesetz ist hierüber die G 10-Kommission zu unterrichten; die durch die Verarbeitung mit Hilfe technischer Systeme erzielten Ergebnisse unterliegen insgesamt den Verarbeitungsregelungen des Artikel 10-Gesetzes. Werden Informationen im Sinne von Satz 2 und 3 in die Informationsverarbeitung einbezogen ist ihre Kennzeichnung nach § 64 Absatz 5 sicherzustellen und aufrechtzuerhalten.“

Auf den Datenumfang begrenzend wirkt sich auch die Regelung in § 69 Abs. 1 Satz 5 LVerfSchG-E aus: „Das Einbeziehen polizeilicher Datenbanken ist unzulässig.“ Es handelt sich hier weniger um ein Problem der Sicherstellung des informatorischen Trennungsgebotes zwischen Nachrichtendiensten und Polizei[40], als ein Problem der hypothetischen Datenneuerhebung. Die Datenübermittlungen von einer operativen Sicherheitsbehörde an einen Nachrichtendienst ist weniger problematisch (als umgekehrt), weil eine Umgehung der verfassungsrechtlichen Anforderungen an den Aufklärungsauftrag der Dienste hier weit weniger naheliegt.[41] Datenbegrenzend und damit eingriffsmildernd wirkt auch § 69 Abs. 1 Satz 6 LVerfSchG-E: „Datensätze aus Internetquellen dürfen einbezogen werden, wenn dies im Einzelfall erforderlich ist.“

[40] BVerfG, Urt. v. 24. 4. 2013 – 1 BvR 1215/07; Bäcker, in: Lisken/Denninger, Handbuch des Polizeirechts, 8. Auflage 2026, Kapitel 2, Rn. 368 f.

[41] Bäcker, in: Lisken/Denninger, Handbuch des Polizeirechts, 8. Auflage 2026, Kapitel 2, Rn. 368 Fn. 692.

Eingriffsmildernd wirkt hier zudem der ausdrückliche Ausschluss einer direkten Anbindung der Analyseplattform an Internetdienste gem. § 69 Abs. 1 Satz 6 LVerfSchG-E: „Ein unmittelbarer automatisierter Abgleich von personenbezogenen Informationen aus Internetdiensten ist unzulässig."

Eingriffsmildernd wirkt zudem § 69 Abs. 5 LVerfGSchG-E zu Informationen von unbeteiligten Dritten: „Durch die IT-gestützte Informationsanalyse gewonnene Informationen zu unbeteiligten Personen dürfen nicht weiterverarbeitet werden.".

Voraussetzung einer begrenzenden Wirkung von Vorgaben zu Art und Umfang der Daten ist, dass die betroffenen personenbezogenen Daten gekennzeichnet werden.[42] § 69 Abs. 4 Satz 5 LVerfSchG-E regelt insoweit: „Werden Informationen im Sinne von Satz 2 und 3 in die Informationsverarbeitung einbezogen ist ihre Kennzeichnung nach § 64 Absatz 5 sicherzustellen und aufrechtzuerhalten."

§ 69 Abs. 8 LVerfSchG-E fordert ein „Rechte- und Rollenkonzept", eine Begrenzung der Nutzerinnen und Nutzer, eine Protkollierung und eine Löschung der Protkolle. Die genaue Ausgestaltung wird hier der Exekutive überlassen. Zwar kann der Gesetzgeber laut BVerfG die entsprechende Regelungsaufgabe auch zum Teil auf die Exekutive übertragen. Er muss aber die wesentlichen Grundlagen zur Begrenzung der Verarbeitungsmethoden und von Art und Umfang der Daten selbst regeln, um dem Gesetzesvorbehalt zu entsprechen.[43] Überträgt der Gesetzgeber der Verwaltung näheres zu regeln, ist eine Verordnungsermächtigung vorzugswürdig.[44]

Die Eingriffsintensität hätte auch noch durch eine Beschränkung der Herkunft der Daten auf solche, die ursprünglich durch inländische Sicherheitsbehörden erhoben worden sind, vorgenommen werden können. Dies ist in § 69 Abs. 1 LVerfSChG-E nicht erfolgt. So könnten auch personenbezogene Daten, die von anderen Geheimdiensten oder von anderen Sicherheitsbehörden der Mitgliedstaaten oder aber von Europäischen Sicherheitsagenturen (wie Europol oder Eurojust) übermittelt wurden und sich somit nunmehr in den polizeilichen Datenbeständen befinden, in eine Analyseplattform nach § 69 Abs. 1 LVerfSChG-E einbezogen werden.

2. Einsatz lernender Systeme

Laut BVerfG verbietet das Grundgesetz lernende Systeme nicht generell.[45] Weil bei selbstlernenden Systemen die Gefahr besteht, dass die demokratische Legitimiationskette zwischen Wahlvolk und Amtswalter und dessen Entscheidungsfindung durchbrochen wird (Demokratieprinzip, Art. 20 Abs. 1, 2 GG), sind dem Einsatz enge Grenzen gesetzt.

In der Literatur wurde angemerkt, dass die technologiebezogenen Aussagen des BVerfG aus dem Jahr 2023 möglicherweise noch unpräzise waren und das Gericht möglicherweise nicht

[42] Ebenso Botta zum ASOG-E, Stellungnahme zum Entwurf eines Gesetzes zur Reform des Berliner Polizei- und Ordnungsrechts und zur Änderung des Gesetzes zu Artikel 29 der Verfassung von Berlin 26.09.2025, S. 14.
[43] BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 110, 112.
[44] BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 113.
[45] BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 100.

zwischen Echtzeitlernmodellen und fixierten Modellen unterschieden hat. Es könne der Eindruck entstehen, das BVerfG habe nur zu Echtzeitlernmodellen urteilen wollen.[46]

§ 69 Abs. 3 S. 1,2,3,4,5 LVerfSchG-E ist dem Wortlaut nach technologieoffen und läßt grundsätzlich den Einsatz selbstlernender Systeme zu. „Die Verfassungsschutzbehörde darf im Rahmen der Informationsverarbeitung nach Absatz 1 Systeme mit mathematisch-statistischen Verfahren, maschinellem Lernen und künstlicher Intelligenz nutzen. In diesem Fall darf die Nutzung von Informationen aus dieser Auswertung durch nicht adaptive Verfahren des maschinellen Lernens und künstlicher Intelligenz nur erfolgen, wenn die Rückschlüsse und die auf ihnen beruhenden Ergebnisse der automatisierten Analyse durch Mitarbeiterinnen und Mitarbeiter der Verfassungsschutzbehörde nachvollzogen und abschließend bewertet werden können. Der Einsatz selbst weiter lernender Systeme ist unzulässig. Eine Verknüpfung der Analysesysteme mit dem Internet erfolgt nicht. Soweit wie technisch möglich, muss die Nachvollziehbarkeit des verwendeten automatisierten Verfahrens zur Informationsverarbeitung und der verwendeten oder relevanten Informationsgrundlagen sichergestellt sein."

Vor dem Hintergrund der Gewährleistung der Menschenwürde (Art. 1 Abs. 1 GG) und dem Demokratieprinzp (Art. 20 Abs. 1, 2 GG) ist es zu begrüßen, dass die Landesregierung die Nachvollziehbarkeitn der Algorithmen und Ergebnisse ausdrücklich verankert. Wegen der Grundrechtsbindung gem. Art. 1 Abs. 3 GG und dem Rechtsstaatsprinzip in Art. 20 Abs. 3 GG muss der Staat sicherstellen, dass staatliche Entscheidungsprozesse nachvollziehbar sind. Die Exekutive könnte ihre Entscheidungen sonst auch nicht hinreichend begründen.[47] § 69 Abs. 3 Satz 6 LVerfSchG-E regelt: „Algorithmen, deren Regeln gruppenbezogenen Merkmalen im Sinne des Artikels 3 Absatz 3 des Grundgesetzes folgen, ohne dass dies durch den Zweck der Informationsauswertung gerechtfertigt ist, dürfen nicht verwendet werden." Wie solche diskriminierende Algorithmen verhindert werden sollen, regelt insbesondere § 69 Abs. 5 Satz 1, 2 LVerfSchG-E: „Eingesetzte IT-Produkte sind regelmäßig zu überprüfen und auf dem Stand der Technik zu halten. Bei der Überprüfung ist auch der Stand der Wissenschaft im Hinblick auf mögliche Angriffe, unerwünschte Veränderungen, Fehler oder Unzulänglichkeiten zu beachten."

Das Eingriffsgewicht sinkt, je „geschlossener" die Methode des Suchvorgangs ist und je stärker die automatisierte Datenanalyse durch polizeiliche Suchmuster gesteuert wird, die auf spezifischen Erkenntnissen und Annahmen zum konkreten Sachverhalt beruhen.[48] In § 69 Abs. 7 LVerfSchG-E heißt es: „Die Entscheidung über den Einsatz von automatisierten technischen Systemen zur Informationsverarbeitung nach Absatz 1, bei denen auch mit nachrichtendienstlichen Mitteln erhobene Informationen verarbeitet werden, trifft die Leitung der Verfassungsschutzabteilung oder ihre Vertretung im Amt. Die Entscheidung ist zu dokumentieren. In ihr sind das Ziel der Informationsauswertung sowie die einzubeziehenden Daten darzustellen." Hier wird der Suchvorgang durch ein Ziel und den Datenumfang beschränkt und damit auch das Eingriffsgewicht.

[46] Etwa Kostov, Der Staat, 64 (2025) 4: 537, 574 f. mit Verweis auf BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 100.
[47] Martini/Botta DÖV 2025, 1033, 1042.
[48] BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 164 ff.

VI. Fazit

Die Landesregierung schlägt mit ihrem Gesetzesentwurf zu Recht eine Modernisierung des LVerfSchG vor. Der Gesetzesentwurf ist auch von dem Anspruch geprägt, die Effektivität der Arbeit des Verfassungsschutzes zu erhöhen, insbesondere auf die rasante Fortentwicklung der Datafizierung der nachrichtendienstlichen Arbeit zu reagieren und zugleich das Verfassungsrecht zu beachten.

Der Entwurf schwächt nur an einigen Stellen die Eingriffsintensität der Maßnahme ab. Ein ganz neuer Eingriff von besonderer Eingriffsintensität bestünde im Anlegen einer neuen vorsorglichen „Superdatenbank". Mangels verfassungsrechtlicher Rechtfertigung wäre eine solche Regelung bereits deshalb verfassungswidrig. Sollte das Anlegen einer vorsorglichen Datenbank gar nicht beabsichtigt sein, müsste dies in der Norm noch klargestellt werden.

Die wesentlichen Leitplanken für Verfahren zur Durchführung der automatisierten Datenanalyse sind durch die Legislative selbst festzulegen. Eine nähere Ausgestaltung kann dann durch die Exekutive erfolgen, insbesondere durch Rechtsverordnungen.

Der Gesetzgeber kann durch Verfahrensanforderungen für Nachvollziehbarkeit, Transparenz und behördliche Kontrolle sorgen, wie etwa mit Pflichten zur Kennzeichnung, Protokollierung oder Benachrichtigung.[49] Dabei gilt, je mehr Daten einbezogen werden (sensible Daten), desto weniger Zugriffsberechtigte sind zulässig. Hier sind Zugriffsbeschränkungen auf einen ausgewählten Kreis mit besonderer Qualifikation erforderlich.[50] Mögliche Vorschriften zu solchen Verfahrensanforderungen wurden im vorliegenden Gesetzesentwurf ohne nähere gesetzliche Maßgaben auf die Exekutive delegiert. Im Sinne der Wesentlichkeitstheorie sind wesentliche Bestimmungen von der Legislative zu treffen. Bei einer Delegation von näheren Vorschriften auf die Exekutive ist eine Verordnungsermächtigung vorzugswürdig.

In einigen Punkten besteht bei der hier betrachteten Ermächtigungsgrundlage zur IT-gestützten Informationsanalyse (§ 69 LVerfG-E) noch Nachbesserungsbedarf. Ich empfehle den Entwurf insoweit entsprechend anzupassen.

gez.

Prof. Dr. iur. Kristin Pfeffer

[49] BVerfG, Urteil v. 16.02.2023 – 1 BvR 1547/19, 1 BvR 2634/20 Rn. 109; Kugelmann/Buchmann, GSZ 2024, S. 1, 9f.
[50] Kugelmann/Buchmann, GSZ 2024, S. 1, 9.