Die neue DNA des Polizeirechts

Automatisierte Datenanalyse als verfassungsrechtliche Herausforderung

Kristin Pfeffer

02.09.2026 doi: 10.59704/acb08b1635715b8f

In Deutschland erlebt das Sicherheitsrecht derzeit eine regelrechte KI-Regulierungsflut. Hierbei wird die automatisierte Datenanalyse in der Gefahrenabwehr und Strafverfolgung etabliert. Der folgende Beitrag gibt einen kurzen Überblick über die rechtlichen Implikationen ihres Einsatzes durch Sicherheitsbehörden und zeigt auf, wo die Defizite der aktuellen Gesetzesentwürfe liegen.

Die automatisierte Datenanalyse ist eine vergleichsweise junge polizeiliche Eingriffsmaßnahme. Sie umfasst die automatisierte Auswertung bereits rechtmäßig erhobener personenbezogener Daten, zum Teil aber auch umfangreicher Datenbestände aus anderen Quellen, wie aus sozialen Netzwerken. Ziel ist es, Sicherheitsbehörden in die Lage zu versetzen, Daten über Beziehungen oder Zusammenhänge zwischen Personen, Personengruppierungen, Organisationen, Institutionen, Objekten und Sachen zu verknüpfen. Hierfür werden Datenanalysesysteme eingesetzt, die die vorhandenen Daten in den polizeilichen Informationssystemen verbinden und unter bestimmten bzw. bestimmbaren Kriterien automatisiert auswerten. Diese sind regelmäßig als Hochrisiko-KI i.S.d. VO (EU) 2024/1689 (KI-VO) einzustufen und unterliegen deshalb besonders umfangreichen Anforderungen der KI-VO. Diese Regulierung durch ein Produktsicherheitsrecht der EU 2024 war aber nur der Anfang: Die KI-VO bedarf im Bereich Hochrisiko-KI mitgliedstaatlicher Umsetzung. Weil die KI-VO außerdem kein Polizeigesetz ist, müssen vor dem Einsatz die entsprechenden Ermächtigungsgrundlagen in den deutschen Sicherheitsgesetzen geschaffen werden. Auch um „den Service" einer automatisierten Datenanalyse durch Europol zu erhalten, benötigen die deutschen Sicherheitsbehörden die gesetzliche Befugnis in ihrem jeweiligen Fachgesetz („Rechtmäßigkeitsfilter"). Das stellt die Gesetzesbegründung[1] zum gerade aktualisierten deutschen Europolgesetz klar.

Europäisierung des Sicherheitsrechts

Das Recht zum Einsatz der automatisierten Datenanalyse durch die Sicherheitsbehörden wurde trotz der Feststellung einer „verfassungsfesten Integrationsschranke" durch das BVerfG[2] und insbesondere, ohne dass das EU-Primärrecht eine Harmonisierung des mitgliedstaatlichen Polizeirechts vorsieht, durch die RL (EU) 2016/680 (DSRL-JI) und die VO (EU) 2024/1689 (KI-VO) teilharmonisiert. Dies ist nicht unumstritten, denn die Annexkompetenz zum Datenschutz aus Art. 16 AEUV dient hier als „Kompetenzsog"[3]. Die DSRL-JI wurde bereits weitgehend umgesetzt, die KI-VO ist gem. Art. 288 AEUV in allen Teilen verbindlich. Im Bereich Polizei- und Strafverfolgungsbehörden sind die Regeln der KI-VO jedoch durch zahlreiche Ausnahmen regelrecht „perforiert" worden. Hier überlässt es der EU-Gesetzgeber im Wesentlichen den Mitgliedstaaten – unter Beachtung des von der KI-VO vorgegebenen verbindlichen Mindeststandards – den Einsatz von KI-Systemen mit Ermächtigungsgrundlagen zu erlauben und noch stärker zu regulieren.

KI-Systeme für die „nationale Sicherheit" fallen schon nach dem Primärrecht nicht in den Anwendungsbereich von Unionsrecht, Art. 4 Abs. 2 Satz 3 EUV (sog. ordre-public-Vorbehalt). Was alles unter „natio-

[1] BT-Drs. 21/2373, https://dserver.bundestag.de/btd/21/023/2102373.pdf, zuletzt abgerufen am 02.09.2026.
[2] BVerfG, 2 BvE 2/06, 2 BvE 5/08, 2 BvR 1010/08, 2 BvR 1022/08, 2 BvR 1259/08, 2 BvR 182/09, 30.06.2009.
[3] Kristin Pfeffer, *Wie europäisch wird deutsches Polizeirecht?: Wie über das Datenschutzrecht die Europäisierung des Polizeirechts betrieben wird*, Verfassungsblog, 28.04.2021, DOI: 10.17176/20210428-173145-0, zuletzt abgerufen am 02.09.2026.

nale Sicherheit" fällt, hat der EuGH[4] bereits geklärt: Es geht hierbei um den Schutz der wesentlichen Funktionen des Staates und der grundlegenden Interessen der Gesellschaft. Ist die automatisierte Datenanalyse auf den Bestandsschutz des Staates gerichtet, wird sie also etwa im Kampf gegen Terrorismus eingesetzt, ist die Befugnisnorm nicht an der KI-VO zu messen.

Vorgaben der KI-VO

Aus der KI-VO ergeben sich umfangreiche Vorgaben für die automatisierte Datenanalyse im Bereich Gefahrenabwehr und Strafverfolgung. Denn eine Software zur automatisierten Datenanalyse gilt dort als Hochrisiko-KI-System i.S.v. Art. 6 KI-VO, gerade weil sie zu bestimmten Einsatzzwecken im Bereich Strafverfolgung oder der straftatenbezogenen Gefahrenabwehr zum Einsatz kommt (Anhang III der KI-VO). Insbesondere die in Anhang III Nr. 6 lit. d und lit. e KI-VO genannten Zwecke werden mit der automatisierten Datenanalyse zur Gefahrenabwehr berührt. Auch dürfte sich regelmäßig ein Profiling oder eine Risikoanalyse anschließen (Anhang III Nr. 6 lit. a). Daraus folgen auf die Produktsicherheit gerichtete Pflichten (Art. 8 ff. KI-VO). Sicherheitsbehörden sind auch dann sog. Quasi-Anbieter, wenn sie ein bereits in Verkehr gebrachtes oder in Betrieb genommenes Hochrisiko-KI-System unter ihrem eigenen Namen bereitstellen, Art. 25 Abs. 1 lit. a KI-VO. So etwa im Fall von „hessenDATA". Sie haben dann zu prüfen, ob der ursprüngliche Anbieter die umfangreichen Pflichten der KI-VO eingehalten hat, und diese künftig selbst zu erfüllen.

Als Verwender von KI-Systemen zur automatisierten Datenanalyse treffen die Sicherheitsbehörden aber vor allem die erheblichen Betreiberpflichten der KI-VO: Sie sind dazu verpflichtet, geeignete technische und organisatorische Maßnahmen zu ergreifen, um die Verwendung des Hochrisiko-KI-Systems nach Maßgabe der Betriebsanleitung sicherzustellen, Art. 26 Abs. 1 KI-VO, und die menschliche Aufsicht einer natürlichen Person mit der erforderlichen Befähigung und Befugnis zu übertragen, Art. 26 Abs. 2 KI-VO. Sie haben sicherzustellen, dass die Eingabedaten relevant und ausreichend repräsentativ sind, Art. 26 Abs. 4 KI-VO. Natürliche Personen sind zu informieren, wenn ein Anhang III-System die betreffenden Entscheidungen trifft oder bei solchen Entscheidungen zur Unterstützung verwendet wird, Art. 26 Abs. 11 KI-VO. Betreiber müssen den Betrieb des Systems überwachen und den Anbieter informieren, wenn sie Grund zur Annahme haben, dass der Einsatz des Systems gemäß der Gebrauchsanweisung die Nonkonformität begründet, Art. 26 Abs. 5 KI-VO. Im Falle eines möglichen Risikos i.S.d. Art. 79 KI-VO ist die zuständige Marktüberwachungsbehörde in Kenntnis zu setzen. Für alle Hochrisiko-KI-Systeme gem. Art. 6 Abs. 2 i.V.m. Anhang III (mit Ausnahme III Ziff. 2 – kritische Infrastrukturen) ist von Polizei- und Strafverfolgungsbehörden eine Grundrechtefolgenabschätzung vorzunehmen. Es besteht eine Registrierungspflicht, Art. 26 Abs. 8 KI-VO. Die KI-Kompetenz der Bediensteten ist zu unterstützen (Art. 4 KI-VO).

Prüfungsmaßstab: Grundgesetz oder Grundrechtecharta?

Ob hier die Grundrechtecharta oder das Grundgesetz Prüfungsmaßstab[5] ist, folgt aus dem Harmonisierungsgrad des mitgliedstaatlichen Sicherheitsrechts. Der ist bei der KI-VO nicht einheitlich zu bestimmen[6]: Im Bereich der sog. Hochrisiko-KI-Systeme nach Art. 6 ff. KI-VO, zu denen die hier behandelte automatisierte Datenanalyse zählt, verbleibt den Mitgliedstaaten nach der KI-VO ein substanzieller Spielraum (Teilharmonisierung). Deshalb bleibt der Prüfungsmaßstab weiterhin das Grundgesetz und nicht die Charta der Grundrechte.[7]

[4] EuGH, *Ligue des droits humains*, C-817/19, 21.06.2022.
[5] S. Fn. 3.
[6] Jason Hofmann-Coombe, *Die Anwendung der Unionsgrundrechte im Polizei- und Sicherheitsrecht nach der KI-VO*, EuR 2025, 363-385 (377) unter Verweis auf BVerfGE 152, 216, 247.
[7] Ebenso Fn. 6 (379); Mario Martini und Jonas Botta, *Polizeiliche Datenanalyse mittels KI – unions-, verfassungs- und polizeirechtliche Leitplanken für Palantir & Co.*, DÖV 2025, 1033-1044 (1040).

Verdachtsgeneratoren ändern die DNA des Polizeirechts

Das BVerfG[8] hat in der sog. Palantir-Entscheidung 2023 festgestellt, dass die automatisierte Datenanalyse vorhandener polizeilicher Daten zum Zweck der Gefahrenabwehr einen neuen, erheblichen Grundrechtseingriff in das Recht auf informationelle Selbstbestimmung darstellt, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. Durch die algorithmische Verknüpfung und Auswertung vorhandener Daten wird neues Wissen generiert, das Rückschlüsse auf betroffene Personen ermöglicht und qualitativ über den ursprünglichen Erhebungszusammenhang hinausgeht. Die besondere Eingriffsintensität ergibt sich aus den der Maßnahme immanenten Belastungseffekten, die unabhängig vom Gewicht der ursprünglichen Datenerhebung bestehen. Die automatisierte Zusammenführung umfangreicher und heterogener Datenbestände verleiht der Maßnahme ein „Eigengewicht". 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. Die Maßnahme wirkt regelmäßig vorgelagert zu weiteren polizeilichen Maßnahmen und beeinflusst die präventive Gefahrenprognose, von der wiederum die Reichweite nachfolgender Eingriffsbefugnisse abhängt. Dadurch wird nicht nur der einzelne Grundrechtseingriff intensiviert. Die Maßnahme wirkt zudem strukturell auf die gesamte Architektur polizeilicher Eingriffsbefugnisse zurück. 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. Klassische Gefahrenprognosen beruhen typischerweise auf einer begrenzten Tatsachengrundlage, die durch menschliche Wahrnehmungs- und Kombinationsfähigkeiten geprägt ist. Automatisierte Analyseverfahren können dagegen vorhandene Datenbestände nahezu augenblicklich verdichten und neue, komplexere Beziehungs- und Verdachtslagen erzeugen. 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.

Das BVerfG[9] bejaht den legitimen Zweck der automatisierten Datenanalyse ebenso wie deren grundsätzliche Geeignetheit und Erforderlichkeit zur vorbeugenden Bekämpfung schwerer Straftaten. Entscheidend ist jedoch die Verhältnismäßigkeit im engeren Sinne. Diese hängt maßgeblich vom Gewicht des Grundrechtseingriffs ab, das das Gericht bei der automatisierten Datenanalyse als besonders hoch einstuft. Vor diesem Hintergrund betont das Gericht implizit, dass bestehende Eingriffsschwellen für polizeiliche Maßnahmen vielfach unter der Prämisse begrenzter menschlicher Auswertungs- und Kombinationsfähigkeiten entwickelt worden seien. Diese Annahme verliert angesichts moderner Analyseverfahren an Tragfähigkeit. In einer zunehmend datafizierten Gesellschaft besteht daher die Gefahr einer strukturellen Ausweitung polizeilicher Eingriffsmöglichkeiten, sofern der Gesetzgeber dem nicht durch klare normative Begrenzungen entgegenwirkt. Die automatisierte Datenanalyse muss 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. Zugleich zeigt das BVerfG auf, dass der Gesetzgeber das Eingriffsgewicht durch verschiedene normative Stellgrößen steuern kann. Dazu zählen insbesondere die Bestimmung der tatbestandlichen Eingriffsschwelle, Regelungen zu Art und Umfang der verarbeitbaren Daten, die Begrenzung besonders sensibler Datenkategorien sowie Vorgaben zur zulässigen

[8] BVerfG, 1 BvR 1547/19, 1 BvR 2634/20, 16.02.2023.
[9] S. Fn. 8.

Methode der Datenanalyse. Ergänzend kommen verfahrensrechtliche Sicherungen in Betracht, etwa Transparenz-, Kennzeichnungs-, Protokollierungs- und Kontrollpflichten. Dabei gilt: Je umfassender und sensibler die einbezogenen Daten sind, desto restriktiver müssen die Zugriffs- und Nutzungsmöglichkeiten ausgestaltet werden. Was den Einsatz selbstlernender Systeme angeht, so war das BVerfG sehr klar:[10]

> *„Wenn der Gesetzgeber die Eingriffsintensität […] reduzieren will, um [die Datenanalyse] auch im Vorfeld einer konkretisierten Gefahr einsetzen zu können, muss er einschränkende Vorgaben zur Methode […] machen. Der Einsatz selbstlernender Systeme muss dafür im Gesetz ausdrücklich ausgeschlossen sein."*

Unklar ist, ob das Gericht hier zwischen Echtzeitlernmodellen und fixierten Modellen differenziert hat.[11]

Kill-Switch beim Nachbarn?

Die öffentliche Debatte um die automatisierte Datenanalyse im Sicherheitsrecht wird derzeit weniger von der Eingriffstiefe der Maßnahme als von der berechtigten Kritik an der Herkunft der eingesetzten Analyseplattformen bestimmt. Da die bisher eingesetzte Software häufig von einem umstrittenen amerikanischen Softwareanbieter stammt, ergeben sich Fragen der technologischen Abhängigkeit sowie der digitalen Souveränität Deutschlands und der Europäischen Union, insbesondere im Hinblick auf Transparenz, Kontrollfähigkeit und langfristige Beherrschbarkeit sicherheitsrelevanter IT-Infrastrukturen. Unterstützt wird diese Forderung inzwischen von der EU. So haben die Mitgliedstaaten am 18. November 2025 die Declaration for European Digital Sovereignty[12] unterzeichnet, wonach Abhängigkeiten zu reduzieren und gemeinsame demokratische Werte im digitalen Raum zu schützen sind.

Regulierungsflut in den Bundesländern

Einige Bundesländer verfügen derzeit über keine spezifische Befugnisnorm für die automatisierte Datenanalyse. Dies gilt für Brandenburg, Bremen, Mecklenburg-Vorpommern und das Saarland. In einigen Bundesländern werden entsprechende Gesetzesvorhaben durchgeführt, etwa in Niedersachsen[13], Schleswig-Holstein[14] und Thüringen[15].

Soweit Bundesländer bereits entsprechende Ermächtigungsgrundlagen haben[16], divergieren diese vor allem im Hinblick auf die methodische Ausgestaltung der Datenanalyse. Während einzelne Länder die Maßnahme auf regelbasierte, deterministische Verfahren beschränken und damit den Einsatz lernender KI-Systeme jedenfalls dem Regelungsziel nach ausschließen, etwa Bayern, Hamburg, Rheinland-Pfalz, Berlin und Sachsen, eröffnen andere Länder einen technikneutralen Regelungsrahmen, der grundsätzlich auch den Einsatz lernender Systeme zulässt, etwa Baden-Württemberg, Hessen, Nordrhein-Westfalen und Sachsen-Anhalt.[17]

Zum Teil soll außerdem der Landesverfassungsschutz eine Ermächtigungsgrundlage zur automatisierten Datenanalyse erhalten, etwa in Schleswig-Holstein.[18]

Novellierung der Bundesgesetze

Der Bundesgesetzgeber hat die automatisierte Datenanalyse zunächst jenseits des klassischen Sicherheitsrechts normativ verankert: In § 29 Abs. 2a Geldwäschegesetz (GwG) und in §§ 2 Abs. 5, 26 Schwarzarbeitsbekämpfungsgesetz (SchwarzArbG).

Aktuelle Gesetzgebungsverfahren sehen die Einführung der automatisierten Datenanalyse in der Strafprozessordnung vor, § 98e StPO-E.[19] Daneben sollen mit dem „Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit"[20] sowie mit dem „Entwurf eines Gesetzes zur Stärkung

[10] S. Fn. 8, Rn. 120.
[11] Etwa Iva Kostov, *Präventive Verhaltensvorhersage durch „künstliche Intelligenz" Möglichkeiten, Maßstäbe, Misstrauen*, Der Staat (2025), S. 537-586 (574 f.9.
[12] Bundesministerium für Digitales und Staatsmodernisierung, *EU-Gipfel: Das war der Gipfel zur europäischen digitalen Souveränität*, 19.11.2025, https://bmds.bund.de/aktuelles/aktuelle-meldungen/detail/eu-summit-das-war-der-gipfel-zur-europaeischen-digitalen-souveraenitaet, zuletzt abgerufen am 02.09.2026.

digitaler Ermittlungsbefugnisse zur Abwehr von Gefahren des internationalen Terrorismus"[21] Befugnisse zur automatisierten Datenanalyse im Bundeskriminalamtsgesetz (BKAG) und im Bundespolizeigesetz (BPolG) verankert werden. Am 29. Juli 2026 hat das Bundeskabinett zudem den Entwurf[22] eines Gesetzes zum Einsatz künstlicher Intelligenz in der Migrationsverwaltung beschlossen, mit dem die Maßnahme in das Asylgesetz (AsylG) und Aufenthaltsgesetz (AufenthG) eingefügt werden soll. Der Gesetzesentwurf[23] zur Reform des Bundesverfassungsschutzgesetzes (BVerfSchG) und des Bundesnachrichtendienstgesetzes (BNDG), vom Bundeskabinett am 12. August 2026 auf den Weg gebracht, sieht die automatisierte Datenanalyse bei den Nachrichtendiensten des Bundes vor.

Europäische Sicherheitsagenturen

Die automatisierten Datenanalysen durch Europol für Mitgliedstaaten sowie für andere EU-Agenturen wie Frontex und Eurojust sind schon etabliert. Allerdings hat die Agentur erst seit 2022 hierfür die gesetzliche Befugnis erhalten, vgl. Änderungsverordnung (EU) 2022/991 zur Verordnung (EU) 2016/794. Dem war eine heftige Auseinandersetzung[24] mit dem Europäischen Datenschutzbeauftragten (EDSB) vorausgegangen.

Fazit

Die automatisierte Datenanalyse ist besonders eingriffsintensiv und ändert den Charakter des Polizeirechts grundlegend. Die Debatte über die US-amerikanische Firma, die das hierbei häufig eingesetzte Analysetool vertreibt, hat diese Tatsache in der Öffentlichkeit etwas überlagert. Währenddessen setzt sich die automatisierte Datenanalyse in den Sicherheitsgesetzen Deutschlands zunehmend als Standardmaßnahme durch, wobei deren Ausgestaltung sehr unterschiedlich erfolgt. Teilweise beschränken sich die Gesetze auf deterministische Verfahren, teilweise ermöglichen sie ausdrücklich den Einsatz lernender Systeme. Insgesamt wenig Eingrenzung erfolgt bei dem Umfang der analysierbaren Daten. Zudem sind die Eingriffsschwellen häufig zu niedrig und die Regelung der Kontrollkonzepte wird vielfach auf die Exekutive delegiert. Weitere Leitplanken des BVerfG sind von den Urteilen zu den Verfassungsbeschwerden zur bayerischen Regelung[25] (Art. 61a Abs. 1 S. 1 BayPAG) und zur hessischen Regelung[26] (§ 25a HessSOG) zu erwarten.

Weil KI-Systeme, die bei der automatisierten Datenanalyse zum Einsatz kommen, sog. Hochrisiko-KI sind, unterliegen Sicherheitsbehörden als Anbieter oder Betreiber komplexen Verfahrensregeln der KI-VO. Mit dem Omnibus zu KI wurde deren Geltung auf den 2. Dezember 2027 verschoben.[27]

Wenig Beachtung wird bisher der Frage geschenkt, in welchem Umfang und für wen die Europäischen Sicherheitsagenturen die automatisierte Datenanalyse anwenden. Der aktuelle Vorschlag[28] der EU-Kommission, das Mandat von Europol grundlegend zu stärken, bietet nun die Gelegenheit, auch die Regelungen zur Durchführung der automatisierten Datenanalyse durch diese Agentur zu überarbeiten.

[13] Niedersächsischer Landtag, Drs. 19/8942, https://www.landtag-niedersachsen.de/drucksachen/drucksachen_19_10000/08501-09000/19-08942.pdf, zuletzt abgerufen am 02.09.2026.
[14] Zeit Online, *Kabinett billigt Gesetzentwurf für mehr Polizeibefugnisse*, 30.03.2026, https://www.zeit.de/news/2026-03/30/kabinett-billigt-gesetzentwurf-fuer-mehr-polizeibefugnisse, zuletzt abgerufen am 02.09.2026.
[15] Thüringer Landtag, Drs. 8/2478, https://parldok.thltcloud.de/parldok/dokument/104845/8_2478_zweites_gesetz_zur_aenderung_des_polizeiaufgabengesetzes, zuletzt abgerufen am 02.09.2026.

AUTOR*IN

Kristin Pfeffer
Kristin Pfeffer ist Professorin für öffentliches Recht an der Hochschule in der Akademie der Polizei Hamburg und Ko-Gründerin der Forschungsstelle Europäisches und Deutsches Sicherheitsrecht (FEDS)

EMPFOHLENE ZITATION

Pfeffer, Kristin: Die neue DNA des Polizeirechts: Automatisierte Datenanalyse als verfassungsrechtliche Herausforderung, Verfassungsblog, 02.09.2026, doi: 10.59704/acb08b1635715b8f.

Lizensiert unter CC BY-SA 4.0.

Langzeitarchiviert bei IntRechtDok unter: doi.org/10.17176/20260902-150512-0.

[16] Für Baden-Württemberg § 47a PolG BW, Bayern § 61a BayPAG, Berlin § 47a ASOG, Hamburg § 49 PolDVG, Hessen § 25a HessSOG, Nordrhein-Westfalen § 23 Absatz 6 PolG NW; Rheinland-Pfalz § 65a POG RhPf; Sachsen § 62a SächsPVDG.

[17] Überblick Mario Martini und Jonas Botta Fn. 7 (1038 ff.); ausführlich Kristin Pfeffer und Luise von Rodbertus, Luise, *Algorithmische Sicherheitsvorsorge – Automatisierte Datenanalyse im nationalen und europäischen Recht*, in: Pfeffer, Kristin (Hrsg.), *AI and Policing in the Security Union – Chancen, Risiken und rechtliche Herausforderungen nach dem AI-Act* (2026), S. 93 ff.

[18] Schleswig-Holsteinischer Landtag, Drs. 20/3754, https://www.landtag.ltsh.de/infothek/wahl20/drucks/03700/drucksache-20-03754.pdf, zuletzt abgerufen am 02.09.2026.

[19] BT-Drs 21/6806, https://dserver.bundestag.de/btd/21/068/2106806.pdf, zuletzt abgerufen am 02.09.2026.

[20] BT-Drs. 21/6132, https://dserver.bundestag.de/btd/21/061/2106132.pdf, zuletzt abgerufen am 02.09.2026.

[21] BT-Drs. 21/6131, https://dserver.bundestag.de/btd/21/061/2106131.pdf, zuletzt abgerufen am 02.09.2026.

[22] Bundesregierung, Entwurf eines Gesetzes zum Einsatz künstlicher Intelligenz in der Migrationsverwaltung, Kabinettsfassung, 29.07.2026, https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/kabinettsfassung/MI6/kimvg-kabinett.pdf?__blob=publicationFile&v=1, zuletzt abgerufen am 02.09.2026.

[23] Bundesregierung, Entwurf eines Gesetzes zur Reform des Bundesverfassungsschutzgesetzes und des Bundesnachrichtendienstgesetzes, Kabinettsfassung, 12.08.2026, https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/kabinettsfassung/OESI2/GE-ND-Reform.pdf?__blob=publicationFile&v=2, zuletzt abgerufen am 02.09.2026.

[24] Europäische Kommission, European Union Agency for Law Enforcement Cooperation (Europol), Zusammenfassung des Rechtsakts, https://eur-lex.europa.eu/DE/legal-content/summary/european-union-agency-for-law-enforcement-cooperation-europol.html, zuletzt abgerufen am 02.09.2026.

[25] Gesellschaft für Freiheitsrechte, Verfassungsbeschwerde gegen Art. 61a Abs. 1 Satz 1 BayPAG, 23.07.2025, https://freiheitsrechte.org/uploads/documents/Freiheit-im-digitalen-Zeitalter/Verfassungsbeschwerde-Art.-61a-BayPAG/2025-07-23-Verfassungsbeschwerde-Art.-61a-BayPAG_geschwaerzt.pdf, zuletzt abgerufen am 02.09.2026.

[26] Gesellschaft für Freiheitsrechte, Verfassungsbeschwerdeschrift gegen § 25a HSOG, 21.07.2024, https://freiheitsrechte.org/uploads/documents/Freiheit-im-digitalen-Zeitalter/Polizeigesetz-Hessen/Verfassungsbeschwerdeschrift-HSOG.pdf, zuletzt abgerufen am 02.09.2026.

[27] Rat der Europäischen Union, *Artificial Intelligence: Council Gives Final Green Light to Simplify and Streamline Rules*, Pressemitteilung, 29.06.2026, https://www.consilium.europa.eu/en/press/press-releases/2026/06/29/artificial-intelligence-council-gives-final-green-light-to-simplify-and-streamline-rules/, zuletzt abgerufen am 02.09.2026.

[28] Europäische Kommission, *Kommission stärkt Europol und Eurojust im Kampf gegen grenzüberschreitende Kriminalität*, Pressemitteilung IP/26/1420, https://ec.europa.eu/commission/presscorner/detail/de/ip_26_1420, zuletzt abgerufen am 02.09.2026.