Deutscher Bundestag **Drucksache 21/6913**

21. Wahlperiode 07.07.2026

Antrag

der Abgeordneten Dr. Konstantin von Notz, Dr. Irene Mihalic, Dr. Lena Gumnior, Marcel Emmerich, Jeanne Dillschneider, Rebecca Lenhard, Helge Limburg, Filiz Polat, Lukas Benner, Schahina Gambir und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Rechtsstaat stärken, Grundrechte schützen – Moderne Polizeiarbeit gestalten

Der Bundestag wolle beschließen:

I. Der Deutsche Bundestag stellt fest:

Die Anforderungen an die deutschen Polizeibehörden haben sich durch Kriminalität, internationale Vernetzung und digitale Kommunikationswege stark verändert. Um Straftaten auch in einer digitalisierten und vernetzten Welt weiterhin wirksam aufzuklären und Gefahren frühzeitig erkennen zu können, benötigen sie moderne technische Ausstattung, zeitgemäße Ermittlungsmethoden und rechtssichere, grundrechtskonforme Einsatzbedingungen. Nur so können sie handlungsfähig gegenüber Kriminellen, Extremisten und staatlichen und quasi-staatlichen Gegnern bleiben, die modernste Technologien gezielt für ihre Zwecke einsetzen.

Handlungsfähigkeit darf jedoch nicht mit der pauschalen Ausweitung von digitalen Ermittlungsbefugnissen gleichgesetzt werden. Die fortschreitende Digitalisierung staatlicher Ermittlungsbefugnisse bringt erhebliche neue Risiken für den Schutz von Bürgerrechten mit sich. Der Schutz der informationellen Selbstbestimmung, die Einhaltung rechtsstaatlicher Sicherungsmechanismen und der durch den Verhältnismäßigkeitsgrundsatz gebotene Verzicht auf ausufernde Massenüberwachung sind eine Stärke unseres demokratischen Rechtsstaats. Vor allem in Zeiten, in denen autoritäre Regimes und andere Feinde der Freiheit im In- und Ausland täglich daran arbeiten, demokratische Regeln zu durchbrechen, freiheitliche Gesellschaftsformen zu destabilisieren, und in denen gerade auch im digitalen Raum autokratische Tendenzen auf dem Vormarsch sind, muss die Bundesrepublik Deutschland ihr freiheitsliebendes Gegenmodell stärken, anstatt selbst Grundrechte abzubauen.

Um dieses freiheitsliebende Gegenmodell weiter zu stärken, ist Digitale Souveränität von entscheidender Bedeutung. Die Hoheit über teils hoch sensible Polizeidaten und zahllose, hoheitlich erhobene, personenbezogene Daten muss bei den Behörden verbleiben und darf nicht an Dritte ausgelagert werden, deren Kontrolle nicht gewährleistet werden kann. Der Einsatz von Produkten nicht vertrauenswürdiger Hersteller wie Palantir muss rechtssicher ausgeschlossen werden.

Um moderne Polizeiarbeit mit Bürgerrechten und höchstrichterlichen Vorgaben in Einklang zu bringen, ist ein Vorgehen mit Augenmaß erforderlich: Neue Technologien dürfen für die Behörden erst nutzbar gemacht werden, nachdem in einem geeigneten Verfahren festgestellt wurde, wie rechtsstaatliche Vorgaben und Si-

cherungsmechanismen mit Bedarfen der Behörden in Einklang gebracht werden können. Dafür braucht es konkrete Vorstellungen von der technischen Umsetzung und der konkreten Datenverarbeitung. Erst dann kann eine tragfähige Rechtsgrundlage geschaffen werden.

Bei der Nutzung von KI ist dabei besonders zu beachten, dass Analysetools nicht nur unmittelbar gesuchte Personen betreffen, sondern aus öffentlich zugänglichen Profilen, Dating-Plattformen oder sogar Falschinformationen oder sexualisierten Deepfakes im Netz auch hoch sensible Informationen über unbeteiligte Dritte gewonnen werden können. Zudem besteht die Gefahr diskriminierender Algorithmen, die unter anderem zu rassistischen Ergebnissen führen können. Neue Befugnisse für die Behörden müssen diese Risiken von vornherein adressieren und Sicherungsmaßnahmen, wie die Verpflichtung zur Erstellung von Schutzkonzepten vor diskriminierenden Algorithmen, umfassende Protokollierungspflichten, Maßnahmen zur Qualitätssicherung oder Transparenz und Nachvollziehbarkeit der Entscheidungsfindung vorsehen.

Das Programm Polizei 20/20 unter Beteiligung aller 20 deutschen Polizeibehörden und der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) spielt bei der Digitalisierung der Polizeiarbeit eine entscheidende Rolle. Das Programm soll das polizeiliche Informationswesen vereinheitlichen, Strukturen, Verfahren und Formate standardisieren und so ein sogenanntes einheitliches polizeiliches Datenhaus schaffen. Das Programm Polizei 20/20 hat das Potential, vorbildhaft zu sein, wenn verfassungsrechtliche Vorgaben zum Schutz der informationellen Selbstbestimmung und IT-Sicherheit by design mitgedacht werden und Polizeibehörden und BfDI von vornherein miteinander daran arbeiten, Freiheit und Sicherheit in einen sachgerechten Ausgleich zu bringen. Der präventiv grundrechtsschonende Ansatz der Entwicklung ist auch deshalb zwingend, weil die ursprüngliche Architektur des „Datenhauses“ durch die Entscheidung des Bundesverfassungsgerichts zum Bundeskriminalamtgesetz (BKAG II) vom 1. Oktober 2024 (Az. 1 BvR 1160/19) wegen unzureichender Sicherheitsvorgaben und erheblicher Mängel bei der Zweckbindung für verfassungswidrig erklärt wurde. Trotz der Dringlichkeit bleibt die Umsetzung des Programms überfällig. Das frustriert nicht nur Ermittlerinnen und Ermittler, sondern bringt die polizeiliche Arbeit im digitalen wie im analogen Raum insgesamt ins Hintertreffen.

Die Bundesregierung hat am 29. April 2026 in mehreren Gesetzesentwürfen Vorschläge vorgelegt, um den Polizeibehörden zum Zweck der Strafverfolgung und den Polizeibehörden des Bundes zur Gefahrenabwehr den biometrischen Abgleich im Internet, die automatisierte Datenanalyse und das Training von KI-Modellen auch mit personenbezogenen Daten zu ermöglichen. Im Rahmen der Länder- und Verbändebeteiligung haben viele Verbände und zivilgesellschaftliche Organisationen massive und grundsätzliche Kritik an den Entwürfen und den geplanten neuen Befugnissen an sich geäußert. Die überwiegende Zahl der Stellungnahmen hält die im Entwurf formulierten Befugniserweiterungen für bürgerrechtlich sehr problematisch und weiten Teilen verfassungs- und unionsrechtswidrig (https://www.bmjv.de/SharedDocs/Downloads/DE/Gesetzgebung/Stellungnahmen/2026/0415_Stellungnahmen_Digitale_Ermittlungsmassnahmen.zip?__blob=publicationFile&v=2) (https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/OESI3/ermittlungsbefugnisse-polizeiarbeit.html). Auch die BfDI weist in ihrer sehr deutlichen Stellungnahme (IA-Drs. 21(4)179) auf die fehlende Vereinbarkeit mit höherrangigem Recht hin und regt an, „alternative Lösungsmöglichkeiten stärker in den Fokus“ zu nehmen.

Die Befugnis zur automatisierten Datenanalyse kann unter Umständen für Sicherheitsbehörden großen Mehrwert bieten und ist in einem begrenzten Umfang für eine zeitgemäße Polizeiarbeit erforderlich. Steigende Datenmengen können ins-

besondere bei umfangreichen Strukturermittlungen dazu führen, dass eine händische Analyse aller relevanten Daten nicht oder kaum noch leistbar ist. Automatisierte Tools können dabei unterstützen, große Datenmengen nach konkreten Begriffen zu durchsuchen, nach Zusammenhängen und Sachverhalten zu clustern und zu sortieren und dadurch auch sehr komplexe Sachverhalte schneller zu bearbeiten und Zusammenhänge herzustellen zu können. Dabei muss unter allen Umständen festgeschrieben und vorhersehbar sein, welche Daten von wem unter welchen Voraussetzungen und zu welchem Zweck wie verarbeitet werden dürfen. Bestehende Dateisysteme dürfen nicht durch die Beschaffung eines Software-Tools gleichsam zu einer zentralen Super-Datenbank zusammengeführt werden. Eine passgenaue IT-Lösung muss datenschutzrechtliche Grundsätze auch zum Zweck der automatisierten Analyse by design mitdenken. Sie muss die differenzierte Rechtsprechung des Bundesverfassungsgerichts (Urteil vom 16. Februar 2023 - 1 BvR 1547/19 - 1 BvR 2634/20 - Automatisierte Datenanalyse) beachten. Je intensiver der Eingriff, desto strenger müssen die Anforderungen an die rechtlichen Sicherungsmaßnahmen und Kontrollmechanismen sein. Zudem darf der Gesetzgeber digitale Analyseinstrumente nicht als Ersatz für eine hinreichend sorgfältige und zweckgebunde Datenverarbeitung missverstehen.

Auch die nachträgliche Identifizierung einzelner verdächtiger Personen zur Bekämpfung schwerster Straftaten durch einen Abgleich im Internet, kann in eng begrenzten und klar geregelten Ausnahmefällen ein wichtiges Instrument für die Sicherheitsbehörden sein. Sie birgt jedoch erhebliche Gefahren für die Grundrechte, auch gänzlich unbeteiligter Personen. Zudem bestehen erhebliche Zweifel an der Vereinbarkeit solcher Verfahren mit geltendem Verfassungs- und Unionsrecht. Demokratien leben von der Verfügbarkeit grundsätzlich unüberwachter öffentlicher Räume, in denen sich Menschen frei bewegen und äußern können, gerade auch im Digitalen. Biometrische Gesichtserkennungssysteme gefährden die relative Anonymität öffentlicher Räume nachhaltig und können sie faktisch beseitigen, unter anderem durch den sog. Chilling Effect. Verfassungsrechtlich folgen aus diesen Grundsätzen höchste Anforderungen an Ermächtigungsgrundlagen für die Sicherheitsbehörden. Auch der europäische Gesetzgeber hat die massiven Gefahren entsprechender Systeme erkannt und in Art. 5 Abs. 1 lit. e der KI-Verordnung (KI-VO) ein Verbot von KI-Systemen, die Datenbanken zur Gesichtserkennung durch das ungezielte Auslesen von Gesichtsbildern aus dem Internet oder von Überwachungsaufnahmen erstellen oder erweitern normiert. Ein Gutachten im Auftrag vom Algorithm Watch (https://algorithmwatch.org/de/wp-content/uploads/2025/10/2025-AW-Gutachten-V9.pdf) geht davon aus, dass es technisch gar nicht möglich ist, Bilder aus dem Internet für einen Abgleich durchsuchbar zu machen, ohne eine solche Datenbank zu erstellen. Darüber hinaus steht in Frage, wie aussagekräftig biometrische Gesichtserkennungssysteme in Zeiten von professionellen Deepfakes noch ist. Die hohe Fehleranfälligkeit stellt den polizeilichen Nutzen in Frage.

Im Kontext digitaler Polizeiarbeit wird immer wieder auch der Einsatz sog. „Intelligenter Videoüberwachung“ diskutiert. Während der Einsatz von KI zur Mustererkennung (etwa, um Massenpanik oder Schlägereien zu erkennen) Mehrwerte in der Gefahrenabwehr bieten kann, stößt die Nutzung von KI-basierter biometrischer Identifikation in öffentlich zugänglichen Räumen – sei sie in Echtzeit oder retrograd – auf erhebliche verfassungsrechtliche Bedenken und schränkt die Grundrechtsausübung im öffentlichen Raum auf unverhältnismäßige Art ein.

Die Entwürfe der Bundesregierung adressieren all diese schwerwiegenden Fragestellungen nicht und verzichten auf notwendige verfassungsrechtliche Sicherungsmechanismen. Anstatt auf die Vereinbarkeit mit der KI-Verordnung einzugehen, ermöglichen die Entwürfe des Bundesinnenministeriums (BMI) es statt-

dessen (vgl. nur § 9a Abs. 5 BKAG-Entwurf) den Behörden, den Abgleich im nicht-europäischen Ausland durchführen zu lassen. Es ist zu befürchten, dass dies ermöglichen soll, den Abgleich durch private Firmen wie PimEyes oder Clearview AI mit Sitz im nichteuropäischen Ausland durchführen zu lassen. Die Geschäftspraktiken beider Firmen sind mit europäischem Recht nicht vereinbar (https://www.inlibra.com/de/document/view/pdf/uuid/45f64af2-47d1-3a7a-bddb-cad625203fa4).

Auch die Vereinbarkeit der geplanten Änderungen in § 15b AsylG mit dem Recht auf Privatsphäre (Art. 7 GrCH und Art. 8 EMRK) steht erheblich in Zweifel. Sie stellen keine bloßen redaktionellen Anpassungen dar, sondern bauen gezielt Schutzvorkehrungen ab und bieten zugleich Rückgriffsmöglichkeiten auf private Anbieter. Die Verhältnismäßigkeit des biometrischem Abgleich zur Identitätsfeststellung steht schon deshalb grundsätzlich in Frage, weil der zugrunde gelegte Identitätsbegriff weit über das hinausgeht, was für das Asylverfahren erforderlich ist (zB Sprachkenntnisse, Ausdruck der kulturellen Identität). Damit wird eine umfassende Ausforschung von Schutzsuchenden legitimiert (siehe gemeinsame Stellungnahme Amnesty, Pro Asyl etc. S. 6 f.). Dabei ist zu beachten, dass Asylsuchende sich auch gegenüber staatlichen Stellen in einer besonders abhängigen Position befinden. Es geht hier nicht um die Aufklärung einer Straftat, sondern ausschließlich um die Feststellung der Identität.

Daneben sehen die Entwürfe der Bundesregierung eine Befugnis vor, hoheitlich erhobene personenbezogene Daten zum Training von KI-Systemen einzusetzen und dafür auch an Private weiterzugeben. Zum Training dürfen auch Daten aus heimlichen Ermittlungsmaßnahmen, wie etwa heimliche Bildaufzeichungen, Telekommunikationsüberwachung oder Daten die durch den Einsatz verdeckter Ermittler gewonnen wurden, verwendet werden. Dies ist mit erheblichen Risiken behaftet und mit datenschutzrechtlichen Grundsätzen unvereinbar.

Im Rahmen des sogenannten „Sicherheitspakets“ hatte die Bundesregierung im Herbst 2024 erstmals Entwürfe für die digitalen Ermittlungsbefugnisse vorgelegt. Die Entwürfe der Bundesregierung wurden den Anforderungen an durchdachte, ausgewogene und mit höherrangigem Recht vereinbare Gesetze nicht gerecht. Die Fraktionen von SPD, FPD und BÜNDNIS 90/DIE GRÜNEN hatten die Entwürfe im parlamentarischen Verfahren vom Kopf auf die Füße gestellt und die Bundesregierung in die Pflicht genommen: So musste das BMI vor Einsatz der neuen Befugnisse in einer Rechtsverordnung hinreichend bestimmt darlegen, wie ein verfassungs- und europarechtskonformer Einsatz überhaupt möglich ist. In einem Entschließungsantrag hat der Deutsche Bundestag die Bundesregierung aufgefordert, bei der Umsetzung auf Hersteller wie Palantir zu verzichten. In der Folge wurden die Gesetze vom Bundesrat abgelehnt, da sie für nicht weitgehend genug befunden wurden.

Auch die Entwürfe der Bundesregierung im Jahr 2026 sind nicht hinreichend durchdacht, nicht bestimmt genug und unausgewogen. Dabei kommt dem Bund bei der Gestaltung digitaler Polizeiarbeit eine Vorreiterrolle zu. Im Rahmen des Programms Polizei 20/20 definiert der Bund der Standards, an denen sich Länder orientieren. Gerade deshalb ist besondere Zurückhaltung bei der Einführung tiefgreifender Befugnisse geboten.Um das Gleichgewicht von Freiheit und Sicherheit zu wahren, erneute Niederlagen vor dem Bundesverfassungsgericht zu vermeiden und grundrechtskonforme, moderne Lösungen zu schaffen, die unseren Sicherheitsbehörden einen echten Mehrwert bieten, braucht es einen anderen Weg. Anstatt gesetzgeberischer Schnellschüsse sollten in einem transparenten Prozess unter Beteiligung von Sicherheitsbehörden, BfDI und dem Bundesamt für Sicherheit in der Informationstechnik (BSI), Zivilgesellschaft und vertrauenswürdigen Herstellern Bedarfe identifiziert, moderne Lösungen erprobt, rechtliche Anforderun-

gen, Grenzen definiert und passgenaue Ansätze entwickelt werden. So können die Behörden mittels neuer digitaler Methoden befähigt und gleichzeitig Transparenz, Vertrauen und Rechtsstaatlichkeit sichergestellt werden. Am Ende eines solchen Prozesses steht die Schaffung passender Rechtsgrundlagen durch den Deutschen Bundestag.

Einen geeigneten Rahmen für einen solchen Prozess können sog. KI-Reallabore bieten. Diese sind rechtlich eingehegte Experimentierfelder, auf denen neue technische Lösungen erprobt werden. Dabei können die Beteiligtengrundrechtsschonend herausfinden, wie nützlich eine Technik wirklich ist und gleichzeitig Antworten auf offene regulatorische Fragen finden. Reallabore können den Weg zu einer grundrechtskonformen, technologisch souveränen und nachhaltigen IT-Infrastruktur für die innere Sicherheit ebnen. Art. 59 Abs. 2 KI-VO eröffnet diese Möglichkeit ausdrücklich auch für den Umgang mit (personenbezogenen) Daten der Sicherheitsbehörden, wenn diese Daten unter der Kontrolle der Behörden verbleiben.

Nach Abwägung aller Umstände kann nur ein solch ausgewogenes Vorgehen Freiheit und Sicherheit in einen sachgerechten Ausgleich bringen und die massiven bürgerrechtlichen Verwerfungen, die das Vorgehen der Bundesregierung mit sich bringt, vermeiden.

II. Der Deutsche Bundestag fordert die Bundesregierung auf,

1) das Projekt Polizei 20/20 mit hoher Priorität voranzutreiben und in enger Zusammenarbeit mit der BfDI und dem BSI darauf hinzuwirken, dass dabei Datenschutzrecht, Transparenz und IT-Sicherheit von vornherein mitgedacht werden;

2) im Rahmen des Projekts Polizei 20/20 Räume zu schaffen, in denen unter Beteiligung von Polizeibehörden, BfDI, BSI, Zivilgesellschaft, Wissenschaft und vertrauenswürdigen Herstellern passgenaue, rechtskonforme und souveräne Lösungen für eine digitale Polizeiarbeit entwickelt und getestet werden, etwa in einem KI-Reallabor gemäß Art. 59 KI-VO;

3) eine Rechtsgrundlage für die automatisierte Datenanalyse erst dann vorzulegen, nachdem in einem Verfahren im Sinne von Forderung Nr. 2 geklärt worden ist, wie technisch, rechtlich und tatsächlich sichergestellt wird, dass die Befugnis wie folgt umgesetzt werden kann:

   a) bestenfalls durch eine Eigenentwicklung, jedenfalls ohne Mitwirkung nicht vertrauenswürdiger Hersteller im nicht-europäischen Ausland wie Palantir,

   b) ohne unregulierten Aufbau einer „Super-Datenbank“, in der Daten aus verschiedenen Informationssystemen unkontrolliert oder zweckentfremdet zusammengeführt werden,

   c) unter Wahrung der Datenhoheit, die jederzeit bei der jeweils zuständigen Polizeibehörde verbleibt,

   d) mit verhältnismäßigen verfassungsrechtlichen Sicherungsmechanismen, die entsprechend der Vorgaben des Bundesverfassungsgerichts je nach Eingriffstiefeintensität differenzierte Voraussetzungen an den Einsatz definieren,

e) mit normenklaren und bestimmen Regelungen, wann welche Daten von wem zu welchem Zweck auf welche Weise verarbeitet werden, sodass jederzeit sichergestellt ist, dass das System ausschließlich solche Daten verarbeitet, die auch ein menschlicher Beamter im konkreten jeweiligen Fall verarbeiten dürfte,

f) sodass die Behörden, Gerichte und die Öffentlichkeit transparent nachvollziehen können, auf welcher Grundlage das System Ergebnisse erzeugt oder Entscheidungen trifft,

g) mit einer Verpflichtung zur Vorlage von Schutzkonzepten zur Vermeidung diskriminierender Entscheidungen,mit spezifischen Kontrollrechten für die Aufsichtsbehörden, die es diesen ermöglichen, nachzuvollziehen, inwieweit die oben genannten Grundsätze in der Praxis eingehalten werden;

4) eine Rechtsgrundlage für den biometrischen Abgleich im Internet nur dann zu schaffen, wenn in einem Verfahren nach Forderung Nr. 2 geklärt wurde, ob und inwieweit technisch, rechtlich und tatsächlich sichergestellt werden kann, dass eine Befugnis nur unter den folgenden Voraussetzungen ausgeübt wird:

a) ohne Aufbau einer biometrischen Datenbank im Sinne von Art. 5 Abs. 1 lit. e KI-VO,

b) bestenfalls durch eine Eigenentwicklung, jedenfalls ohne Mitwirkung nicht vertrauenswürdig Hersteller mit Sitz im nicht-europäischen Ausland wie Palantir, PimEyes oder Clearview,

c) unter Wahrung der Datenhoheit, die jederzeit bei der jeweils zuständigen Polizeibehörde verbleibt,

d) mit verhältnismäßigen verfassungsrechtlichen Sicherungsmechanismen, insbesondere der Voraussetzung eine qualifizierten Verdachts oder der drohenden Gefahr einer besonders schweren Straftat nach § 100b Abs. 2 StPO und eines Richtervorbehalts,

e) mit Einschränkungen des Anwendungsbereichs, die das Eingriffsgewicht der Maßnahme verringern, etwa der Beschränkung auf bestimmte Teile des Internets und einem eingeschränkten Adressatenkreis,

f) mit spezifischen Kontrollrechten für die Aufsichtsbehörden, die es diesen ermöglichen, nachzuvollziehen, inwieweit die oben genannten Grundsätze in der Praxis eingehalten werden;

5) die Verwendung von KI-basierter biometrischer Identifikation in öffentlich zugänglichen Räumen (intelligente Videoüberwachung) in Echtzeit und retrograd auszuschließen;

6) das Training von Künstlicher Intelligenz mit hoheitlich erhobenen personenbezogenen Daten zu unterlassen;

7) sich auf Ebene der Europäischen Union dafür einzusetzen, dass die bestehenden Vorgaben der KI-VO für den Einsatz von KI in Sicherheitsbehörden nicht abgesenkt oder aufgeweicht werden;

8) wissenschaftlich unabhängig zu prüfen, inwieweit an Kriminalitätsschwerpunkten die sog. Mustererkennung mittels KI einen Mehrwert in der Gefahrenabwehr bringt, der die damit verbundenen starken Eingriffe rechtfertigen kann;

9) die Befugnis zum biometrischen Abgleich durch das Bundesamt für Migration und Flüchtlinge zum Zweck der Identitätsfestellung grundsätzlich zu streichen;

Berlin, den 7. Juli 2026

Katharina Dröge, Britta Haßelmann und Fraktion