



Stellungnahme der Gewerkschaft der Polizei (GdP)

zu den Referentenentwürfen des
Bundesministeriums des Innern

**Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse
in der Polizeiarbeit (Teil 1) sowie zur Abwehr von Gefahren des inter-
nationalen Terrorismus (Teil 2)**

Berlin, 01.04.2026
Abt. Innenpolitik | 31, AL3

I. - Vorbemerkung

Die Gewerkschaft der Polizei (GdP) begrüßt, dass mit den vorliegenden Gesetzentwürfen die digitalen Ermittlungsbefugnisse der Sicherheitsbehörden des Bundes weiterentwickelt und an die tatsächlichen Bedingungen moderner Gefahrenabwehr und Strafverfolgung angepasst werden sollen. Die zunehmende Verlagerung von Kriminalität in den digitalen Raum stellt die Polizeibehörden seit Jahren vor erhebliche tatsächliche und rechtliche Herausforderungen. Dies gilt in besonderem Maße für die Bekämpfung schwerer und grenzüberschreitender Kriminalität, bei denen Identitätsfeststellung, Aufenthaltsermittlung und sachverhaltsbezogene Auswertung digitaler Spuren eine wachsende Rolle spielen. Der gesetzgeberische Ansatz, diesen Entwicklungen mit ausdrücklichen Befugnissen für den automatisierten biometrischen Abgleich mit öffentlich zugänglichen Daten aus dem Internet sowie für die automatisierte Datenanalyse zu begegnen, ist deshalb im Ausgangspunkt richtig und erforderlich.

Dabei kommt es nicht allein auf die Schaffung neuer Befugnisse an. Entscheidend ist, dass diese Befugnisse im Vollzug rechtssicher, praxistauglich und gerichtsfest ausgestaltet werden. Unklare Eingriffsschwellen, unbestimmte Begriffe, unzureichend strukturierte Verfahrensregeln oder technisch nicht hinreichend eingehegte Anwendungen führen in der Praxis nicht zu mehr Sicherheit, sondern zu Rechtsunsicherheit, zusätzlichem Rechtfertigungsdruck, Beweisverwertungsrisiken und letztlich auch zu Belastungen unserer eingesetzten Kolleg:innen. Die Aufgabe des Gesetzgebers besteht deshalb nicht nur darin, neue Ermittlungsinstrumente zu eröffnen, sondern diese so zu normieren, dass ihre Anwendung nachvollziehbar, kontrollierbar und in gerichtlichen Verfahren belastbar bleibt.

Die Gewerkschaft der Polizei (GdP) - mit über 210.000 Mitgliedern größte Polizeigewerkschaft hierzulande - begrüßt diesen richtigen und wichtigen Schritt und bedankt sich für die Gelegenheit zu diesem sicherheitspolitisch wichtigen Vorhaben Stellung zu nehmen.

II. - Zum Vorhaben

Die GdP begrüßt ausdrücklich, dass das Bundesministerium des Innern (BMI) mit dem vorliegenden Entwurf den im Impulspapier der Gewerkschaft der Polizei (GdP) zur Bundestagswahl 2025 formulierten Vorschlag¹ aufgreift und nun den Vorstoß wagt, die rechtlichen Voraussetzungen für den nachträglichen biometrischen Abgleich mit öffentlich zugänglichen Daten aus dem Internet zu schaffen. Damit setzt das BMI ein wichtiges Signal, dass die Praxisimpulse der Polizei ernst genommen werden, und stärkt zugleich die Fähigkeit der Sicherheitsbehörden, schwere und schwerste Straftaten effektiv und rechtsstaatlich kontrolliert zu bearbeiten.

Die vorgesehenen Befugnisse tragen einem praktischen Bedarf Rechnung, der sich aus der digitalen Realität moderner Sicherheitsarbeit ergibt. Sie sollen es ermöglichen, vorhandene Erkenntnisse in gewichtigen Fällen schneller, strukturierter und zielgerichteter auszuwerten. Gerade im Bereich der Terrorismusbekämpfung und schwerer Kriminalität kann dies für die Identifizierung relevanter Personen, die Ermittlung von Aufenthaltsorten und die Erkennung von

¹ Vgl. GdP (2024): Die Innere Sicherheit Deutschlands wirksam stärken. Impulse der Gewerkschaft der Polizei (GdP) zur Bundestagswahl 2025, S. 5. Abrufbar unter: <https://www.gdp.de/Bundesvorstand/Dokumente/Impulspapiere/GdP-Impulse-zur-BTW-2025.pdf>.

Zusammenhängen von erheblicher Bedeutung sein. Ebenso nachvollziehbar ist der Ansatz, automatisierte Datenanalyse dort zu ermöglichen, wo bereits rechtmäßig zugängliche Datenbestände strukturiert zusammengeführt und ausgewertet werden müssen, um schwere Kriminalität, konkretisierte Gefahrenlagen oder terroristische Bedrohungen wirksamer zu erkennen und zu bearbeiten. Gerade in komplexen, arbeitsteiligen oder grenzüberschreitenden Lagen kann eine solche technische Unterstützung von erheblichem praktischem Nutzen sein.

Neue digitale Ermittlungsmaßnahmen können allerdings nur dann Akzeptanz beanspruchen, wenn gesetzlich und organisatorisch sichergestellt ist, dass sensible Daten ausschließlich anlassbezogen, streng zweckgebunden, nachvollziehbar und in einem auf das absolut Erforderliche beschränkten Umfang verarbeitet werden. Gerade aus Sicht der GdP ist dies kein Hemmnis effektiver Sicherheitsarbeit, sondern ihre Voraussetzung. Der vorliegende Entwurf enthält insoweit wichtige Ansatzpunkte. Dazu gehören insbesondere die Beschränkung auf öffentlich zugängliche Internetdaten, der Ausschluss von Echtzeitdaten, qualifizierte Eingriffsschwellen, Subsidiaritätsanforderungen, Löschungs- und Protokollierungspflichten, technische und organisatorische Schutzmaßnahmen sowie die ausdrückliche Vermeidung ausschließlich automatisierter belastender Entscheidungen. Ein datensicher und normenklar ausgestalteter Rechtsrahmen schützt nicht nur Betroffene, sondern auch die handelnden Behörden und Beschäftigten vor Rechtsunsicherheit, Legitimationsdruck und späteren Beanstandungen.

Für die GdP ist in diesem Zusammenhang ein weiterer Grundsatz besonders wichtig: Digitale Ermittlungsinstrumente können polizeiliche und behördliche Arbeit unterstützen, strukturieren und beschleunigen, sie dürfen die eigenverantwortliche menschliche Bewertung und Entscheidung aber nicht ersetzen. Technische Systeme können Hinweise verdichten, Zusammenhänge sichtbar machen und Entscheidungsgrundlagen aufbereiten. Die Verantwortung für Bewertung, Gewichtung und Folgemaßnahmen muss jedoch stets beim handelnden Menschen verbleiben. Dieser Grundsatz ist für die rechtsstaatliche und praktische Akzeptanz des gesamten Vorhabens zentral.

Aus Sicht der GdP gehört zur rechtssicheren und praxistauglichen Ausgestaltung digitaler Ermittlungsbefugnisse jedoch nicht nur eine klare gesetzliche Ermächtigungsgrundlage, sondern auch eine belastbare, souveräne und sicherheitsgerechte technische Umsetzungsarchitektur. Wo der Gesetzgeber auf digitale Ermittlungsinstrumente und Analyseplattformen abstellt, muss zugleich sichergestellt sein, dass diese Systeme dauerhaft unter behördlicher Kontrolle stehen, höchsten Anforderungen an Datensicherheit und Vertraulichkeit genügen und nicht in technische oder organisatorische Abhängigkeiten führen, die dem Anspruch staatlicher Souveränität widersprechen.

III. - Im Einzelnen

1. Zum automatisierten biometrischen Abgleich mit öffentlich zugänglichen Daten aus dem Internet (§§ 9a, § 39a, 63b BKAG-E, § 58a BPolG-E, § 15b AsylG-E)

Die in den Entwürfen vorgesehenen Befugnisse zum automatisierten biometrischen Abgleich mit öffentlich zugänglichen Daten aus dem Internet sind aus Sicht der GdP grundsätzlich zu begrüßen. Der Gesetzgeber trägt damit dem Umstand Rechnung, dass Identifizierung, Aufenthaltsermittlung und Zusammenhangsermittlung in der heutigen Sicherheits- und

Ermittlungsarbeit vielfach nicht mehr ohne digitale Bezugspunkte erfolgen können. Das Instrument kann insbesondere dazu beitragen, bislang unbekannte Personen zu identifizieren, Hinweise auf ihren Aufenthaltsort zu gewinnen und bereits vorhandene Ansätze in gewichtigen Fällen zu verdichten.

Positiv hervorzuheben ist, dass die Entwürfe den biometrischen Abgleich nicht anlasslos eröffnen, sondern an qualifizierte Voraussetzungen binden. Erforderlich sind jeweils konkretisierte Verdachts- oder Gefahrenlagen, gewichtige Schutzgüter oder erhebliche Straftaten sowie die Feststellung, dass die Maßnahme für Identifizierung, Aufenthaltsermittlung, Sachverhaltsaufklärung oder Zusammenhangsermittlung erforderlich ist. Ebenso ist die Beschränkung auf öffentlich zugängliche Internetdaten sachgerecht. Sie verdeutlicht, dass zwischen allgemein zugänglichen digitalen Inhalten und geschützten privaten Kommunikations- und Rückzugsräumen unterschieden wird. Dass Echtzeitdaten ausdrücklich ausgeschlossen werden, unterstreicht zusätzlich den begrenzten und nachträglichen Charakter der Maßnahme.

Von besonderer Bedeutung ist aus Sicht der GdP, dass diese Regelungen den Umgang mit biometrischen Daten betreffen und damit mit Daten von besonderer Sensibilität. Gerade deshalb ist es richtig, dass die Entwürfe auf Zweckbindung, Löschung, Protokollierung und Datensicherheit abstellen. Die vorgesehene Begrenzung auf verfahrens- oder aufgabenbezogene Nutzung, die unverzügliche Löschung nicht weiter benötigter Daten, die Einbeziehung technischer und organisatorischer Schutzmaßnahmen sowie die Protokollierung der Verarbeitungsschritte stärken die Nachvollziehbarkeit und die rechtsstaatliche Einhegung der Maßnahme.

Die Absätze 5 und 6 der jew. Ges-E eröffnen schließlich die Möglichkeit, den biometrischen Abgleich durch externe Stellen durchführen zu lassen, sofern dies technisch erforderlich ist. Während Absatz 5 dies für inländische sowie unionsrechtliche Stellen regelt, enthält Absatz 6 besondere Voraussetzungen für die Einbindung von Stellen in Drittstaaten, insbesondere das Erfordernis des Schutzes der nationalen Sicherheit sowie die Einhaltung mit Ausnahmen datenschutzrechtlicher Vorgaben. Für letztgenannte Fälle sieht bspw. § 9a Abs. 8 BKAG-E einen Richtervorbehalt vor, der lediglich bei Gefahr im Verzug durch eine behördliche Anordnung ersetzt werden kann, wobei eine gerichtliche Bestätigung binnen drei Tagen nachzuholen ist. Hierzu stellt die GdP fest, dass diesen Regelungen in der Praxis insbesondere so lange eine hohe Bedeutung zukommen wird, da die technischen Fähigkeiten zur Durchführung der Maßnahmen vielfach insbesondere bei Dritten vorhanden sind, die außerhalb der EU ansässig sind. Vor diesem Hintergrund ist der notwendige inhärent herzustellende Bezug zur „nationalen Sicherheit“ von herausgehobener Bedeutung. Jedoch darf dieser in der Praxis aber nicht so eng ausgelegt werden, dass er polizeiliches Tätigwerden durch Anwendung der in Abs. 6 vorgesehenen, für die Praxis gegenwärtig herausragend bedeutsamen Maßnahmen, verunmöglicht. Mit Blick auf die nahe Zukunft unterstützt die GdP alle Bestrebungen der technischen Weiterentwicklung im Sinne der Schaffung digitaler Souveränität, die dazu führen, dass die Praxisrelevanz der Regelung nach Abs. 6 alsbald minimiert werden.

Bedauerlich ist in diesem Zusammenhang aus unserer Sicht zudem, dass es BMI und BMJV offenkundig nicht gelungen ist, einen Gleichklang der vorgesehenen Regelungen in den parallel

laufenden, inhaltlich verschränkten polizeigesetzlichen (BMI)² bzw. strafprozessualen (BMJV)³ Gesetzesvorhaben herzustellen. Das Vorsehen des Erfordernisses eines Richtervorbehaltes im gegenständlichen BMI-Vorhaben erscheint vor dem Hintergrund des Verzichts auf ebenjenes im § 98d Abs. 4 StPO-E (BMJV-Vorhaben) nicht nur systematisch fragwürdig. Er dürfte auch die polizeiliche Praxis unnötig erschweren und ist somit abzulehnen.

2. Zur automatisierten Datenanalyse (§§ 9b, 39b, 63c BKAG-E, § 58b BPolG-E)

Auch die vorgesehenen Regelungen zur automatisierten Datenanalyse sind aus Sicht der GdP zu begrüßen. Moderne Sicherheitsarbeit ist in schweren und komplexen Lagen zunehmend darauf angewiesen, rechtmäßig zugängliche Datenbestände nicht nur nebeneinander vorzuhalten, sondern strukturiert, sachverhaltsbezogen und technisch unterstützt auszuwerten. Recherche- und Analyseplattformen können dazu beitragen, Zusammenhänge früher zu erkennen, relevante Hinweise zusammenzuführen und Ermittlungs- oder Gefahrenabwehrmaßnahmen zielgerichteter auszurichten. Ihr Mehrwert liegt in der strukturierten Aufbereitung bereits vorhandener Daten, nicht in der Schaffung unkontrollierter neuer Datenbestände.

Zugleich ist gerade im Bereich der automatisierten Datenanalyse hervorzuheben, dass die Zusammenführung und Auswertung unterschiedlicher Datenbestände die Eingriffsintensität deutlich steigern kann. Umso wichtiger ist, dass die Entwürfe die Maßnahme an qualifizierte Schwellen binden, den Funktionsumfang beschreiben, offene anlasslose Suchen ausschließen und klarstellen, dass die Analyseplattform die Arbeit der Behörden unterstützt, aber nicht an die Stelle eigenverantwortlicher Bewertung tritt. Besonders zu begrüßen ist in diesem Zusammenhang der ausdrückliche Ausschluss ausschließlich automatisierter belastender Entscheidungen. Damit wird der für die GdP zentrale Grundsatz aufgenommen, dass am Ende stets der Mensch die Entscheidung trifft und technische Systeme nur eine unterstützende Funktion erfüllen dürfen.

Auch hier ist der Schutz sensibler Daten von zentraler Bedeutung. Wo unterschiedliche Datenbestände zusammengeführt, analysiert, gewichtet, visualisiert und statistisch ausgewertet werden, steigen die Anforderungen an Datensicherheit, Zugriffsbegrenzung, Protokollierung und organisatorische Absicherung zwingend an. Positiv ist daher, dass der Entwurf besondere Schulungsanforderungen, technische und organisatorische Schutzmaßnahmen, Protokollierungspflichten sowie die Beachtung allgemeiner datenschutzrechtlicher Anforderungen vorsieht. Diese Elemente sind aus Sicht der GdP wesentlich, um die praktische Nutzbarkeit und die rechtsstaatliche Akzeptanz der Analyseinstrumente dauerhaft zu sichern.

Aus Sicht der GdP kommt es hierbei entscheidend darauf an, dass die gesetzlich eröffneten Analysebefugnisse mit einer tragfähigen und nachvollziehbaren Umsetzungsstruktur verbunden werden. Soweit der Entwurf auf Analyseplattformen Bezug nimmt, sollte der weitere Gesetzgebungs- und Umsetzungsprozess erkennen lassen, in welcher organisatorischen und technischen Grundstruktur diese Instrumente betrieben und fortentwickelt werden sollen. Für die Praxis ist wesentlich, dass Zuständigkeiten, Verantwortlichkeiten und Betriebsstrukturen klar, einheitlich und nachhaltig angelegt sind. Gerade im Interesse von Standardisierung, Interoperabilität und

² Siehe gegenständliche Referentenentwürfe des BMI.

³ Siehe Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz (BMJV): Entwurf eines Gesetzes zur Änderung der Strafprozessordnung – digitale Ermittlungsmaßnahmen.

Verfahrenssicherheit spricht viel dafür, entsprechende Lösungen zentral und behördenübergreifend konsistent zu denken.

3. Zur Weiterverarbeitung von Daten für Entwicklung, Überprüfung, Änderung und Training von IT-Produkten (§ 22 BKAG n.F., § 46 BPolG n.F.)

Die vorgesehenen Ergänzungen zur Weiterverarbeitung von Daten für Entwicklung, Überprüfung, Änderung und Training von IT-Produkten trägt einem praktischen Bedarf Rechnung, der mit der zunehmenden Digitalisierung sicherheitsbehördlicher Arbeit an Bedeutung gewinnt. Wenn IT-Produkte, Analysewerkzeuge oder selbstlernende Systeme im sicherheitsbehördlichen Bereich wirksam, belastbar und praxistauglich eingesetzt werden sollen, bedarf es auch einer rechtssicheren Grundlage für Entwicklung, Überprüfung und Anpassung. Dass der Entwurf hierfür eine ausdrückliche spezialgesetzliche Grundlage schaffen will, ist zu begrüßen und gibt der Praxis Rückendeckung für ihr Tätigwerden. Zugleich ist zu begrüßen, dass der Entwurf die besondere Sensibilität solcher Datenverarbeitungen erkennt und sie an Zweckbindung, Erforderlichkeit sowie besondere Geheimhaltungs- und Schutzvorgaben bindet. Gerade wenn Echtdaten für Entwicklungs- oder Testkontexte genutzt werden, muss jederzeit sichergestellt sein, dass Datensicherheit, Vertraulichkeit und Kontrolle in besonderem Maße gewahrt bleiben.