21. Wahlperiode

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache 21(4)214 F
vom 18. September 2026

Schriftliche Stellungnahme

von Martina Link, Vizepräsidentin des Bundeskriminalamts vom 17.9.2026

zu dem

a) Gesetzentwurf der Bundesregierung
Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse zur Abwehr von Gefahren des internationalen Terrorismus
BT-Drucksachen 21/6131, 21/7265

b) *Gesetzentwurf der Bundesregierung*
Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit
BT-Drucksachen 21/6132, 21/6511

c) Gesetzentwurf der Bundesregierung
Entwurf eines Gesetzes zur Änderung der Strafprozessordnung – digitale Ermittlungsmaßnahmen
BT-Drucksache 21/6806

d) Antrag der Abgeordneten Dr. Konstantin von Notz, Dr. Irene Mihalic, Dr. Lena Gumnior, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN
Rechtsstaat stärken, Grundrechte schützen – Moderne Polizeiarbeit gestalten
BT-Drucksache 21/6913

e) Antrag der Abgeordneten Clara Bünger, Donata Vogtschmidt, Luke Hoß, weiterer Abgeordneter und der Fraktion Die Linke
Nein zu biometrischen Massenerkennungssystemen
BT-Drucksache 21/6917

Bundeskriminalamt

Bundeskriminalamt • 65173 Wiesbaden

Deutscher Bundestag
Innenausschuss
Platz der Republik 1
11011 Berlin

Am Treptower Park 5-8
12435 Berlin

Zentrale Postanschrift:
65173 Wiesbaden

Tel. 0611-55 0
Fax +49 611 55-26003

bearbeitet von:
Leitungsstab 4

www.bka.de

Anhörung zur Stärkung digitaler Ermittlungsbefugnisse am 21.09.2026
hier: Stellungnahme des BKA

Wiesbaden, 17.09.2026

<u>Vorbemerkung und grundsätzliche Bewertung:</u>

Polizeiliche Arbeit ist einem kontinuierlichen Wandel unterworfen. Technologische Entwicklungen, veränderte Kommunikations- und Lebensgewohnheiten sowie die zunehmende Digitalisierung nahezu sämtlicher Lebensbereiche wirken sich unmittelbar auf die Art und Weise aus, in der Straftaten begangen, vorbereitet und verschleiert werden. Die Polizei muss bei der Gefahrenabwehr und Strafverfolgung auf diese Entwicklungen angemessen reagieren können. Dies setzt voraus, dass die hierfür zur Verfügung stehenden rechtlichen und technischen Instrumente fortlaufend weiterentwickelt werden.

Eine besondere Herausforderung stellt die stetig wachsende Menge digital verfügbarer Informationen dar. Dies betrifft sowohl die im Internet öffentlich zugänglichen Informationen als auch die Datenbestände, die die Polizeibehörden im Rahmen konkreter Ermittlungsverfahren erlangt haben, etwa aus sichergestellten Smartphones oder anderen digitalen Datenträgern. Die Verarbeitung und Auswertung dieser Datenmengen sind ein wesentlicher Bestandteil polizeilicher Ermittlungsarbeit. Die damit verbundenen Herausforderungen können nicht allein durch eine entsprechende Ausweitung personeller Ressourcen bewältigt werden. Vielmehr bedarf es geeigneter technischer Verfahren, um rechtmäßig erhobene und vorhandene Informationen effizient zu erschließen und für die polizeiliche Aufgabenwahrnehmung nutzbar zu machen.

Die vorgesehene Regelung für die **automatisierte Datenanalyse** versetzt das BKA in die Lage, große und komplexe Datenbestände strukturiert auszuwerten, Zusammenhänge zwischen Personen, Sachverhalten, Orten oder Ereignissen zu erkennen und hieraus belastbare Ermittlungsansätze zu gewinnen. Die automatisierte Datenanalyse stellt damit ein Instrument zur Unterstützung der polizeilichen Sachbearbeitung dar, mit dem vorhandene Informationen effizienter erschlossen werden können.

Die Befugnis für einen **automatisierten biometrischen Abgleich** ermöglicht es dem BKA, mit Hilfe öffentlich zugänglicher Daten aus dem Internet Hinweise zur Identität, zum Aufenthaltsort von Personen sowie zu möglichen Tat-Täter-Zusammenhängen zu gewinnen. Die Suche nach der Person „Daniela Klette“ in 2024 hat gezeigt, dass eine derartige Befugnis wesentliche neue Ermittlungs- und Fahndungsansätze ermöglichen würde, die anders nicht erzielt werden könnten.

Für das Bundeskriminalamt sind diese Befugnisse sowohl als Ermittlungsbehörde als auch im Rahmen seiner Aufgabenwahrnehmung als Zentralstelle von erheblicher Bedeutung.

Die vorgesehenen Verfahren sollen bei der polizeilichen Aufgabenwahrnehmung insbesondere dazu dienen, die Sachverhaltsaufklärung zu unterstützen, Ermittlungsansätze zu generieren und die Entscheidungsgrundlage der zuständigen Ermittlerinnen und Ermittler zu verbessern. Die Verantwortung für die polizeiliche Bewertung und die daraus abzuleitenden Maßnahmen verbleibt dabei beim Menschen; eine eigenständige, unmittelbar rechtsfolgenauslösende Entscheidung durch ein technisches System ist gerade nicht Gegenstand der vorgesehenen Befugnisse.

Von besonderer praktischer Bedeutung ist darüber hinaus die Befugnis zum Erlass von Sicherungsanordnungen für Verkehrsdaten gegenüber den Telekommunikations-diensteanbietern. Gerade bei digitalen Spuren kommt dem zeitlichen Faktor besondere Bedeutung zu, da entsprechende Daten regelmäßig nur für begrenzte Zeit verfügbar sind. Die Sicherungsanordnung ermöglicht die erforderliche zeitliche Überbrückung zwischen dem Bekanntwerden eines relevanten Sachverhalts und dem Vorliegen der tatsächlichen und rechtlichen Voraussetzungen für eine spätere Datenerhebung. Für das Bundeskriminalamt ist dies insbesondere im Rahmen seiner Zentralstellenfunktion von Bedeutung, da hierdurch eine zeitnahe und effektive Sicherung relevanter Verkehrsdaten auch in Sachverhalten ermöglicht wird, bei denen die örtliche Zuständigkeit noch zu klären sind.

Schließlich stellt die nach dem Gesetzentwurf zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit ausdrücklich normierte Möglichkeit, KI-basierte und sonstige IT-Produkte anhand bereits beim Bundeskriminalamt vorhandener Echtdaten zu testen und zu trainieren, einen elementaren Bestandteil des Gesetzespakets dar. Die praktische Entwicklung und Erprobung solcher Produkte ist erforderlich, um deren Einsatzmöglichkeiten, Leistungsfähigkeit und Grenzen unter realitätsnahen Bedingungen beurteilen und die Systeme im weiteren Verlauf sachgerecht fortentwickeln zu können. Hierbei ist gerade eine Verwendung von Echtdaten ein zentrales Element, um eine in der Praxis belastbare Einschätzung der Eignung der zu erprobenden IT- und/oder KI-Anwendungen für die jeweiligen polizeilichen Einsatzszenarien zu ermöglichen. Anwendungs- und datenspezifische Besonderheiten sowie mögliche Fehlerquellen können so frühzeitig erkannt und unter realistischen Bedingungen bewertet werden.

1. Automatisierte Datenanalyse

Gerade die besondere verfassungsrechtliche Rolle des Bundeskriminalamtes als Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen und für die Kriminalpolizei erfordert hohe Fähigkeiten im Bereich der Auswertung und Analyse von Daten. Als Zentralstelle hat das Bundeskriminalamt den gesetzlichen Auftrag, Informationen zu sammeln und auszuwerten und muss daher mit den rechtlichen sowie technischen Mitteln ausgestattet werden, die es in die Lage versetzen, diesen Auftrag bestmöglich zu erfüllen.

Stetig wachsende, enorme Datenmengen (Massendaten), stellen in Bezug auf die Auswertefähigkeiten des Bundeskriminalamts eine der größten bzw. schwierigsten Herausforderungen dar. Eine händische Auswertung dieser Datenmengen ist nicht nur ineffizient, sie ist tatsächlich nicht mehr praktikabel, da sie zu viel Zeit und Ressourcen in Anspruch nimmt. Vielfältige Medienbrüche, also die Wechsel zwischen verschiedenen Datenquellen oder -formaten, erschweren diese Arbeit zudem erheblich, da sie eine konsistente und durchgängige Analyse behindern. Ein weiteres Problem stellt das Erkennen von fallübergreifenden Zusammenhängen dar, die aufgrund ihrer Komplexität und der Menge der Daten oft schwer oder gar nicht zu erfassen sind. Schließlich besteht aufgrund der verschärften Sicherheitslage ein hoher Zeit- und Handlungsdruck, der eine schnelle und zuverlässige Analyse der Daten erfordert, damit die Polizei im Rahmen von Strafverfolgung und Gefahrenabwehr angemessen reagieren kann.

Die neue Befugnis zur automatisierten Datenanalyse soll es dem Bundeskriminalamt ermöglichen, bereits rechtmäßig von ihm gespeicherte Daten und solche, auf die es rechtmäßig zugreifen kann, mit technischen Mitteln auszuwerten und zu analysieren.

Die gesetzlich vorgesehenen Voraussetzungen und die Bindung an den jeweils im Einzelfall zu begründenden polizeilichen Aufgabenzweck stellen dabei sicher, dass verfassungsrechtliche Grundsätze gewahrt bleiben.

Hierbei wird auch die vom Bundesverfassungsgericht hervorgehobene Unterscheidung zwischen der Begrenzung der einzubeziehenden Daten und der Eingriffsschwelle für die Durchführung der Analyse berücksichtigt. Die Befugnis knüpft nämlich nicht nur an den jeweils bestehenden Datenzugriff an, sondern setzt für ihre konkrete Nutzung zusätzliche aufgaben- und eingriffsbezogene Voraussetzungen voraus. Die automatisierte Analyse ersetzt damit weder die polizeiliche Verantwortungsentscheidung noch die erforderliche Prüfung der Verhältnismäßigkeit im Einzelfall durch den Ermittler oder Ermittlerin.

Ferner regeln die vorliegenden Gesetzentwürfe – unter Berücksichtigung der verfassungsgerichtlichen Rechtsprechung – explizit, welche Daten in die automatisierte Datenanalyse einbezogen werden dürfen. Das Bundeskriminalamt kann nur Daten einbeziehen, die ihm bereits bekannt sind; genannt werden insbesondere polizeiliche Auskunftssysteme und der Informationsverbund, Vorgangs- und Falldaten, Asservatendaten sowie Telekommunikations-, Verkehrs- und Nutzungsdaten. Ergänzend können Datensätze aus gezielten Abfragen in staatliche Register sowie einzelne, bereits gespeicherte Datensätze, z.B. aus Internetquellen (bspw. sichergestellte Videos mit konkreten Anschlagsdrohungen seitens bekannter extremistischer Gruppierungen), einbezogen werden.

Insofern eröffnet die Datenanalysebefugnis dem Bundeskriminalamt lediglich die Möglichkeit, bereits rechtmäßig erlangte Daten automatisiert auszuwerten. Dies wird zusätzlich dadurch verdeutlicht, dass eine direkte Anbindung der Analyseanwendung an bestimmte externe Register und Internetdienste ausdrücklich ausgeschlossen ist. Daten aus externen Quellen können nur im konkreten Einzelfall einbezogen werden, wenn sie zuvor aufgrund einer entsprechenden Befugnisnorm rechtmäßig erhoben wurden und rechtmäßig gespeichert bzw. zwischengespeichert vorliegen.

Zudem wird in den jeweiligen Befugnisnormen ausdrücklich auf § 12 BKAG verwiesen. Damit findet – entsprechend der Systematik des BKAG – eine weitere Eingrenzung der einzubeziehenden Daten statt, nicht nur über die jeweilige Befugnisnorm, sondern auch anhand der entsprechenden Grundsätze der hypothetischen Datenneuerhebung und der Zweckbindung. Zusätzlich werden über weitere Verweisungsnormen Daten zur Vorgangsverwaltung und zur befristeten Dokumentation polizeilichen Handelns sowie darüber hinaus auch Daten, die den Kernbereich privater Lebensgestaltung betreffen, explizit vom Anwendungsbereich der Vorschrift ausgenommen.

Für die Durchführung einer automatisierten Datenanalyse ist eine Zusammenführung der entsprechenden Daten auf einer Analyseplattform vorgesehen, die sowohl einzelfallbezogen als auch einzelfallunabhängig erfolgen und insbesondere hinsichtlich des Grunddatenbestands auch eine dauerhafte Zusammenführung ermöglichen kann; die Plattform kann dabei als eine Art Arbeitsspeicher bzw. temporäre Arbeits- oder Analyseumgebung verstanden werden. Die gesetzlichen Speicher- und Aussonderungsfristen der in die Analyse einbezogenen Daten sowie die sonstigen datenschutzrechtlichen Vorgaben bleiben unberührt und gelten auch bei möglichen technischen Redundanzen. Entscheidend ist daher zwischen der bestehenden rechtmäßigen Speicherung der Ausgangsdaten und der lediglich technisch erforderlichen Zusammenführung für die Analyse zu unterscheiden.

Im Fokus der automatisierten Datenanalyse steht, durch die Analyse und Verknüpfung von Informationen Tat-Täter-Zusammenhänge herzustellen.
Ein praktisches Beispiel hierfür ist die Auswertung umfangreicher Datenbestände in einem Verfahren wegen des Verdachts der Vorbereitung eines terroristischen Anschlags. Werden etwa Vorgangs- und Falldaten, Erkenntnisse aus sichergestellten digitalen Datenträgern sowie bereits rechtmäßig vorliegende Telekommunikations- und Nutzungsdaten zusammengeführt, kann eine automatisierte Analyse bislang nicht erkennbare Verbindungen zwischen Personen, Kommunikationsvorgängen, Orten und Zeitpunkten sichtbar machen. Hierdurch können sich beispielsweise Hinweise darauf ergeben, dass mehrere bislang getrennt betrachtete Sachverhalte mit denselben Personen oder Infrastrukturen in Zusammenhang stehen.

Dass sich in den hierbei verarbeiteten, rechtmäßig vorhandenen Daten auch Informationen zu Opfern, Zeugen oder sonstigen unbeteiligten Personen befinden können, lässt sich bei komplexen Sachverhalten nicht vollständig vermeiden. Ihre bloße Einbeziehung in eine Analyse macht diese Personen jedoch weder zu Verdächtigen noch löst sie automatisch weitere Maßnahmen aus. Die Ergebnisse der Analyse sind daher als Erkenntnisquelle zu

verstehen, die von den zuständigen Polizeibeamten bewertet und in den jeweiligen Sachzusammenhang eingeordnet werden muss. Insbesondere bei Maßnahmen mit unmittelbaren Auswirkungen auf Betroffene bleibt eine eigenständige rechtliche und tatsächliche Bewertung durch die zuständigen Ermittlerinnen und Ermittler erforderlich.

Technische Analyseverfahren sind zudem so einzusetzen, dass die geltenden rechtlichen Anforderungen an eine sachgerechte und diskriminierungsfreie Aufgabenwahrnehmung eingehalten werden. So verlangt bereits die KI-VO, dass mögliche Verzerrungen untersucht und geeignete Maßnahmen zu ihrer Erkennung, Validierung und Abschwächung getroffen und im Rahmen von Validierungs- und Testverfahren potentiell diskriminierende Auswirkungen berücksichtigt werden. Dies ist nicht nur über die Bestimmungen der KI-VO, sondern auch über eine direkte Verankerung in den Vorschriften des vorliegenden Gesetzesentwurfs sichergestellt. Gekoppelt mit der zwingend vorgeschriebenen abschließenden Bewertung und Entscheidung durch geschulte Sachbearbeiterinnen und Sachbearbeiter stellt dies sicher, dass diskriminierende und intransparente Entscheidungen vermieden werden.

2. Biometrischer Internetabgleich

Das Bundeskriminalamt bewertet die vorgesehene Befugnis zum automatisierten biometrischen Abgleich mit öffentlich zugänglichen Daten aus dem Internet aus kriminalfachlicher Sicht als ein zeitgemäßes und für seine Aufgabenwahrnehmung erforderliches Ermittlungsinstrument. Die zunehmende Verlagerung relevanter Informationen in den digitalen Raum eröffnet auch für die kriminalpolizeiliche Sachverhaltsaufklärung neue Informationsquellen, die mit herkömmlichen Ermittlungsansätzen nicht oder nur eingeschränkt erschlossen werden können. Dies gilt insbesondere für öffentlich zugängliche Bild- und Videodaten, anhand derer sich Hinweise zur Identität, zum Aufenthaltsort von Personen sowie zu möglichen Tat-Täter-Zusammenhängen gewinnen lassen.

Der biometrische Internetabgleich ermöglicht es, bereits vorliegende Ermittlungsansätze gezielt mit öffentlich verfügbaren Informationen abzugleichen und dadurch bestehende Erkenntnisse zu verdichten.
Ausgangspunkt kann beispielsweise das Lichtbild einer gesuchten oder tatverdächtigen Person sein. Ein automatisierter Abgleich mit öffentlich zugänglichen Bild- und Videodaten kann zusätzliche Hinweise auf die Identität oder den Aufenthaltsort der betreffenden Person liefern oder Verbindungen zu weiteren Personen, Sachverhalten oder kriminellen beziehungsweise terroristischen Strukturen aufzeigen.

Ein praktischer Anwendungsfall besteht etwa bei der Fahndung nach einer Person, die im Zusammenhang mit einem schweren Gewalt- oder Terrorismusdelikt steht und deren aktueller Aufenthaltsort unbekannt ist. Liegt den Ermittlungsbehörden ein Lichtbild der Person vor, könnte dieses automatisiert mit öffentlich zugänglichen Bild- und Videodaten abgeglichen werden. Wird die Person beispielsweise auf einem öffentlich zugänglichen Bild oder in einem öffentlich verfügbaren Video an einem bislang unbekannten Ort erkannt, kann dies einen konkreten Hinweis auf ihren aktuellen oder jüngeren Aufenthaltsort liefern und zugleich weitere Ermittlungsansätze eröffnen.

Voraussetzung für die Anwendung der vorgesehenen neuen Befugnis sind daher bestehende strafrechtliche Ermittlungen beziehungsweise eine konkretisierte Gefahrenlage. Darüber hinaus ist der Einsatz des biometrischen Abgleichs auf Straftaten von erheblicher Bedeutung begrenzt und gegenüber anderen geeigneten Maßnahmen subsidiär ausgestaltet. Der Abgleich ist an konkrete gesetzliche Voraussetzungen – abhängig vom jeweils im Rahmen des Aufgabenspektrum des Bundeskriminalamts verfolgten polizeilichen Zweck – gebunden und soll insbesondere die Identifizierung von Tatverdächtigen oder Störern oder deren Aufenthaltsermittlung in besonders gewichtigen Fällen ermöglichen. Auch hier gilt: Das technische Ergebnis ist kein selbständiger Beweis oder eine automatische Entscheidung, sondern bedarf vor belastenden Folgemaßnahmen der Prüfung und Bewertung durch die zuständigen Polizeibeamtinnen und Polizeibeamten.

Die Befugnis ist dabei ausdrücklich auf öffentlich verfügbare und damit jedermann zugängliche Daten beschränkt. Nicht erfasst sind insbesondere Daten, die nur einem abgegrenzten Personenkreis zugänglich sind, private Kommunikation über Messenger-Dienste sowie Daten, die zum Zeitpunkt des Abgleichs ein tatsächliches Geschehen in Echtzeit wiedergeben. Eine Echtzeitüberwachung des öffentlichen Raumes ist damit vom Anwendungsbereich der Regelung nicht umfasst.

Darüber hinaus befürwortet das Bundeskriminalamt gerade die in den jeweiligen Vorschriften gewählte technikoffene Formulierung ausdrücklich. Diese ist erforderlich, weil sich biometrische Identifizierungstechnologien schnell weiterentwickeln und neue Verfahren hinzukommen können. Eine abschließende Aufzählung einzelner biometrischer Merkmale würde daher Gefahr laufen, bereits bei Inkrafttreten des Gesetzes technisch überholt zu sein. Vergleichbare gesetzliche Regelungstechniken finden sich auch im Strafverfahrensrecht, wo die Befugnisse ebenfalls nicht auf eine einzelne konkrete technische Ausgestaltung beschränkt, sondern bewusst technikoffen formuliert werden. Begrenzungen erfolgen deshalb vorrangig über den Zweck, die Eingriffsvoraussetzungen und die Art der zulässigen Verarbeitung.

Des Weiteren begrüßt das Bundeskriminalamt insbesondere, dass die Gesetzentwürfe zum BKAG eine rechtssichere und zugleich KI-VO- sowie europarechts- und datenschutzkonforme Einbindung privater Anbieter in die Durchführung des biometrischen Internetabgleichs ermöglichen. Dies ermöglicht, für die praktische Umsetzung auf spezialisierte technische Lösungen Dritter zurückzugreifen. Die vorgesehenen Regelungen schaffen aus Sicht des Bundeskriminalamtes damit einen geeigneten rechtlichen Rahmen für eine technisch zeitgemäße und zugleich rechtskonforme Zusammenarbeit mit privaten Anbietern.
Unter den bestehenden hohen Anforderungen stellt dies aus Sicht des Bundeskriminalamtes die grundrechtsschonendste Variante eines entsprechenden Abgleichs dar. Eine massenhafte Sammlung und Speicherung öffentlich zugänglicher Bilder durch eine Sicherheitsbehörde ist so nicht notwendig.
Soweit der Gesetzentwurf die Nutzung entsprechender Systeme eines in einem Drittland angesiedelten privaten Anbieters erlaubt, gilt dies nur im Rahmen der Bereichsausnahme des

Art. 2 Abs. 3 KI-VO - also für Fälle, die die nationale Sicherheit betreffen. Damit ist ein Verstoß gegen die KI-VO sowie sonstige europarechtliche Bestimmungen nicht gegeben.

Im Übrigen ist darauf hinzuweisen, dass die Voraussetzungen für einen biometrischen Internetabgleich im Falle der Nutzung eines privaten Anbieters in einem Drittland weitestgehend den Voraussetzungen für eine Öffentlichkeitsfahndung entsprechen. Aus Sicht des Bundeskriminalamtes handelt es sich bei der Öffentlichkeitsfahndung um eine weitaus eingriffsintensivere Maßnahme. Während bei der Öffentlichkeitsfahndung nämlich Abbildungen des Betroffenen einer breiten Öffentlichkeit zugänglich gemacht werden, werden Abfragen bei privaten Anbietern nur einem eng begrenzten Kreis bekannt. Darüber hinaus können derartige Anfragen äußerst grundrechtsschonend ausgestaltet werden, indem sie legendiert über einen anonymen Account, d.h. ohne Offenlegung des polizeilichen Hintergrunds, vorgenommen werden.

Insgesamt begrüßt das Bundeskriminalamt daher die vorgesehene Schaffung einer ausdrücklichen Rechtsgrundlage für den automatisierten biometrischen Abgleich mit öffentlich zugänglichen Daten aus dem Internet. Aus Sicht des BKA könnten diese Regelungen vor dem Hintergrund der aktuellen Bedrohungs- und Sicherheitslage noch effizienter und zugleich europarechts- und verfassungskonform ausgestaltet werden.
Zum einen regt das Bundeskriminalamt eine Prüfung an, warum für die Anwendung des biometrischen Internetabgleichs ein Richtervorbehalt erforderlich ist, obwohl die Eingriffstiefe geringer ist als bei einer Öffentlichkeitsfahndung.
Darüber hinaus sollte den Ermittlerinnen und Ermittlern in den Ländern eine eigene Möglichkeit der Abfrage in Drittstaaten in der StPO eingeräumt und so der bislang vorgesehene Umweg über das BKA überflüssig gemacht werden. Dies würde einen erheblichen Effizienzgewinn bedeuten.

3. Sicherungsanordnungen

Eine Befugnis zur Sicherungsanordnung von Verkehrsdaten bei Anbietern von Telekommunikationsdiensten verhindert im Einzelfall einen vorzeitigen Datenverlust. Dies gilt nicht nur bei der Strafverfolgung (StPO), sondern auch nach dem Gesetzentwurf zum BKAG für die Aufgaben des BKA in seinen Aufgaben nach §§ 2 (Zentralstelle) und 5 BKAG (Abwehr von Gefahren des internationalen Terrorismus).

Diese Befugnis für das BKA als Zentralstelle ist wegen der Flüchtigkeit oder Nichtspeicherung von Verkehrsdaten notwendig. Die Sicherungsanordnung der Zentralstelle soll hierbei gewährleisten, dass während der Klärung der örtlichen, polizeilichen Zuständigkeit für den Sachverhalt relevante Daten zwischenzeitlich nicht den Löschroutinen der TK-Anbieter unterfallen. Die Löschung der Daten könnte in der Folge die Identifizierung des Störers oder des Tatverdächtigen und somit die Aufklärung des Sachverhaltes verhindern.

Ein typischer Anwendungsfall ist etwa ein zunächst nicht eindeutig zuordenbarer Hinweis auf eine geplante schwere Straftat. Gehen Informationen ein, wonach über einen bestimmten Internetanschluss oder eine bestimmte Telefonnummer eine für die Gefahrenabwehr oder Strafverfolgung relevante Kommunikation stattgefunden haben könnte, steht zu diesem Zeitpunkt möglicherweise noch nicht fest, welche Polizeibehörde örtlich oder sachlich

zuständig ist oder ob die rechtlichen Voraussetzungen für eine Erhebung der Verkehrsdaten bereits vorliegen. Durch eine Sicherungsanordnung kann in dieser Zwischenphase verhindert werden, dass die beim Telekommunikationsdiensteanbieter vorhandenen relevanten Verkehrsdaten aufgrund regulärer Löschfristen verloren gehen. Nach Klärung der Zuständigkeit und des weiteren Vorgehens können die Daten dann – soweit die hierfür erforderlichen gesetzlichen Voraussetzungen vorliegen – auf Grundlage der einschlägigen Befugnisnorm erhoben werden.

Die Einführung einer neuen Befugnis etwa zur Erhebung der Daten durch das BKA als Zentralstelle ist mit dieser Anpassung nicht verbunden. Die Daten werden aufgrund der Verfügung durch den TK-Anbieter lediglich vorläufig gesichert. Sofern die Datenerhebung im weiteren Verlauf erforderlich ist, erfolgt dies auf Basis des bestehenden Gefahrenabwehrrechts der Länder oder je nach Lage des Sachverhaltes z. B. auch nach dem BKAG (Aufgabe nach § 5 BKAG).

Aus denselben Gründen - um eine Löschung identifizierungsrelevanter Verkehrsdaten zu verhindern - ist die Sicherungsanordnung auch für die BKA-Aufgabe der Abwehr von Gefahren des internationalen Terrorismus erforderlich. Es gibt Gefahrensachverhalte, in denen die rechtlichen Voraussetzungen für eine Verkehrsdatenerhebung noch nicht vorliegen, also noch keine bestimmten Tatsachen, sondern lediglich Anhaltspunkte dafür vorliegen, dass eine Person für eine Gefahr verantwortlich ist, deren Verkehrsdaten für die Abwehr der Gefahr von Bedeutung sein können. Für diese Konstellation soll zumindest die Sicherung der Daten vor ihrer Löschung greifen, um eine vollständige spätere Verkehrsdatenerhebung abzusichern.
In konkreten Gefahrensachverhalten, die in den Ländern bearbeitet werden, muss eine derartige Sicherungsanordnung ebenfalls möglich sein. Hierzu bedarf es noch der zeitnahen rechtlichen Fixierung einer sog. Länderöffnungsklausel in § 176 Abs. 1 TKG-E, damit gewährleistet ist, dass Sicherungsanordnungen nach den Polizeigesetzen der Länder künftig ebenfalls zulässig sind.

4. Testen und Trainieren von IT-Systemen

Bei der Befugnis zum Testen und Trainieren von IT-Systemen (§ 22 BKAG-E) handelt es sich nicht um eine eigenständige Ermittlungsbefugnis, sondern um eine notwendige technische Voraussetzung für die sichere, zuverlässige und funktionsfähige Wahrnehmung polizeilicher Aufgaben mit modernen IT- und KI-Systemen. Die Befugnis dient ausschließlich den Zwecken des Testens und Trainierens und ist damit von der unmittelbaren operativen Aufgabenerfüllung klar abzugrenzen.

Aus fachlicher Sicht ist eine solche Regelung insbesondere deshalb erforderlich, weil IT-Systeme vor ihrer Inbetriebnahme und auch während ihres Einsatzes im Wirkbetrieb umfassend auf ihre Funktionsfähigkeit und Zuverlässigkeit überprüft werden müssen. Neue Funktionen oder Änderungen an bestehenden Systemen können regelmäßig nicht unmittelbar im produktiven Betrieb erprobt werden, ohne die Sicherheit und Funktionsfähigkeit der polizeilichen Informationsverarbeitung zu beeinträchtigen. In der Praxis kann es daher erforderlich sein, Echtdaten für Testzwecke in einer gesicherten Testumgebung zu verwenden. Die vorgesehene Regelung schafft hierfür einen klaren und

rechtssicheren Rahmen und vermeidet zugleich eine aufwändige Herleitung der Zulässigkeit aus allgemeinen datenschutzrechtlichen Vorschriften.

Das Testen dient dabei nicht allein der technischen Qualitätssicherung. Eine sorgfältige Erprobung ist auch erforderlich, um fehlerhafte oder verzerrte Verarbeitungsergebnisse frühzeitig zu erkennen und dadurch insbesondere ungerechtfertigte oder diskriminierende Ergebnisse sowie eine fehlerhafte Belastung oder Nichtentlastung einzelner Personen zu vermeiden. Mit geeigneten Tests werden zudem Sicherheitslücken, unberechtigte Zugriffsmöglichkeiten und potenzielle Systemausfälle erkannt und können vor einem Einsatz im Wirkbetrieb behoben werden. Das Testen von IT-Systemen ist damit zugleich ein wesentlicher Bestandteil eines verantwortungsvollen und grundrechtsschonenden Einsatzes datenverarbeitender Technologien.

Auch das Trainieren von KI-Systemen bietet für die kriminalpolizeiliche Aufgabenwahrnehmung einen erheblichen Mehrwert. Durch das Training werden Leistungsfähigkeit und Zuverlässigkeit KI-gestützter Systeme verbessert. Dies trägt dazu bei, polizeiliche Ressourcen gezielter einzusetzen und die Qualität der kriminalistischen Sachbearbeitung zu erhöhen.
So kann eine entsprechend trainierte KI beispielsweise bei der strukturierten Aufbereitung umfangreicher Erkenntnisse zu Personen oder Sachverhalten unterstützen und etwa eine chronologisch geordnete Gesamtschau vorhandener Informationen erstellen. Bevor ein solches System im Wirkbetrieb eingesetzt werden kann, muss anhand geeigneter Echtdaten überprüft werden, ob es relevante Informationen zuverlässig erkennt, Informationen zutreffend zuordnet und etwaige systematische Fehl- oder Verzerrungseffekte bestehen. Werden dabei Fehler festgestellt, kann das System in einer gesicherten Testumgebung angepasst und erneut überprüft werden. Gleiches gilt für die Weiterentwicklung eines bereits eingesetzten Systems, etwa wenn dieses künftig umfangreichere oder anders strukturierte Daten verarbeiten soll. Die Verwendung von Echtdaten ermöglicht dabei eine realitätsnahe Überprüfung, die mit rein künstlich erzeugten Testdaten nicht in gleicher Weise gewährleistet werden kann.

Aus Sicht des Bundeskriminalamtes ist es sachgerecht, dass die vorgesehene Regelung unter bestimmten Voraussetzungen auch die Einbindung externer Stellen ermöglicht. Dies ist insbesondere dann erforderlich, wenn für die Entwicklung, Erprobung oder Optimierung eines IT- oder KI-Systems besondere technische Expertise außerhalb des Bundeskriminalamtes vorhanden ist oder entsprechende Arbeiten im Rahmen der europäischen und internationalen Zusammenarbeit, etwa mit anderen Sicherheitsbehörden, erforderlich sind. Die Übermittlung personenbezogener Daten an Dritte ist dabei keineswegs voraussetzungslos möglich, sondern unterliegt definierten Schutzmechanismen.

Hierzu zählt insbesondere der Ausschluss besonders eingriffsintensiv erhobener personenbezogener Daten, die strikte Zweckbindung in Bezug auf das Testen oder Trainieren sowie die Vorgabe, dass eine Verwendung durch Dritte ausschließlich zu den vom Bundeskriminalamt vorgegebenen Zwecken erfolgen darf. Zudem ist die Übermittlung auf Personen beschränkt, die aufgrund ihrer Stellung oder besonderer gesetzlicher beziehungsweise dienstlicher Verpflichtungen zur Wahrung der Vertraulichkeit verpflichtet

sind. Soweit Echtdaten an Dritte zu nichtpolizeilichen Zwecken übermittelt werden, ist darüber hinaus im Rahmen der gesetzlich vorgesehenen Ermessensentscheidung stets die Verhältnismäßigkeit der konkreten Übermittlung zu prüfen.

Das Bundeskriminalamt bewertet die vorgesehenen Befugnisse zum Testen und Trainieren von IT-Systemen insgesamt als wichtigen Baustein für eine sichere und zukunftsfähige Digitalisierung der kriminalpolizeilichen Aufgabenwahrnehmung. Sie ermöglicht es, die für den Einsatz moderner IT- und KI-Systeme notwendige technische Qualitätssicherung und Weiterentwicklung rechtssicher durchzuführen, ohne die für die Verarbeitung personenbezogener Daten geltenden Schutzanforderungen abzusenken.

Fazit:
Das Bundeskriminalamt begrüßt die mit den Gesetzentwürfen vorgesehene Schaffung und Konkretisierung der entsprechenden Befugnisse. Sie schaffen die notwendige rechtliche Grundlage dafür, die Möglichkeiten moderner Datenverarbeitung und KI-gestützter Verfahren dort nutzbar zu machen, wo dies zur effektiven Wahrnehmung der gesetzlichen Aufgaben erforderlich ist, und tragen damit zu einer zeitgemäßen und zukunftsfähigen Ausgestaltung der polizeilichen Arbeit bei.
Mit den Befugnissen erhält das Bundeskriminalamt die rechtlichen Möglichkeiten, mit dem zunehmend im digitalen Raum stattfindenden Kriminalitätsgeschehen Schritt halten zu können. Konkrete Verbesserungsvorschläge hat das BKA in Bezug auf den biometrischen Internetabgleich und in Bezug auf die Sicherungsanordnung dargestellt.