

BDK | Wollankstraße 135 | D-13187 Berlin

An das Bundesministerium des Innern
Alt Moabit 140
10557 Berlin

Per Mail: OeSI3@bmi.bund.de

Bundsvorsitzender

Ansprechpartner/in: Dirk Peglow
Funktion: Bundsvorsitzender

E-Mail: dirk.peglow@bdk.de
Telefon: +49 30 2463045-0

Datum: 06.04.2026

Stellungnahme des Bund Deutscher Kriminalbeamter e. V. (BDK) zu den Referentenentwürfen des Bundesministeriums des Innern zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit sowie zur Abwehr von Gefahren des internationalen Terrorismus

1. Ausgangslage und sicherheitspolitischer Kontext

Der Bund Deutscher Kriminalbeamter e.V. (BDK) begrüßt die vorliegenden Referentenentwürfe ausdrücklich. Sie greifen eine Entwicklung auf, die die kriminalpolizeiliche Praxis seit Jahren prägt und deren Dynamik weiter zunimmt. Kriminalität ist heute in weiten Teilen digital organisiert, international vernetzt und arbeitsteilig strukturiert. Insbesondere im Bereich der schweren und organisierten Kriminalität sowie des internationalen Terrorismus entstehen komplexe Täter- und Unterstützungsstrukturen, die sich klassischen Ermittlungsansätzen zunehmend entziehen. Parallel hierzu wächst die Menge der in Ermittlungs- und Gefahrenabwehrverfahren verfügbaren Daten kontinuierlich an. Diese Daten liegen jedoch häufig unstrukturiert, verteilt über unterschiedliche Systeme und „Datentöpfe“ und ohne unmittelbare Verknüpfbarkeit vor. Das zentrale Problem moderner Polizeiarbeit besteht daher nicht im Mangel an Informationen, sondern in deren fehlender Auswertbarkeit.

Die vorliegenden Referentenentwürfe des Bundesministeriums des Innern sind dabei nicht isoliert zu betrachten. Sie stehen in einem engen inhaltlichen Zusammenhang mit einem parallel vorgelegten Referentenentwurf des Bundesministeriums der Justiz zur Stärkung digitaler Ermittlungsbefugnisse in der Strafprozessordnung, zu dem zeitgleich eine gesonderte Verbändeanhörung durchgeführt wird.

Beide Vorhaben verfolgen erkennbar eine gemeinsame Zielrichtung, nämlich die Stärkung der Fähigkeit staatlicher Sicherheitsbehörden, vorhandene Datenbestände effektiver zu nutzen und moderne digitale Analyseinstrumente rechtlich abzusichern.

Während der Entwurf des Bundesministeriums der Justiz primär die strafprozessuale Ebene adressiert, betreffen die hier vorliegenden Entwürfe die präventiv-polizeilichen Befugnisse sowie die Rolle des Bundeskriminalamtes als Zentralstelle. Aus Sicht des BDK ist es daher von besonderer Bedeutung, beide Gesetzgebungsvorhaben als Teil eines einheitlichen Gesamtansatzes zu betrachten und in ihrer praktischen Wirkung aufeinander abzustimmen.

2. Wandel der kriminalpolizeilichen Erkenntnisgewinnung

Vor diesem Hintergrund setzen die Gesetzentwürfe an der entscheidenden Stelle an. Sie tragen dem Umstand Rechnung, dass kriminalpolizeiliche Erkenntnisgewinnung heute maßgeblich durch die strukturierte Nutzung bereits vorhandener Daten bestimmt wird. Der entscheidende Fortschritt liegt nicht mehr allein in der Erhebung neuer Informationen, sondern in der Fähigkeit, vorhandene, rechtmäßig erhobene und gespeicherte Daten zusammenzuführen, zu analysieren und in einen sinnvollen Gesamtzusammenhang zu stellen.

Die vorgesehenen Befugnisse zur automatisierten Datenanalyse greifen diese Entwicklung auf und schaffen eine notwendige gesetzliche Grundlage für ein Instrument, das in der Praxis längst als unverzichtbar angesehen wird. Sie ermöglichen es, komplexe Datenbestände systemübergreifend auszuwerten, Zusammenhänge sichtbar zu machen und daraus neue Erkenntnisse zu gewinnen, die mit herkömmlichen Methoden nicht erreichbar wären. Die Beschränkung auf bereits rechtmäßig erhobene Daten sowie der Ausschluss automatisierter Entscheidungen mit unmittelbarer Rechtswirkung tragen dabei den verfassungsrechtlichen Anforderungen Rechnung und schaffen eine tragfähige Balance zwischen Effektivität und Grundrechtsschutz.

3. Biometrischer Internetabgleich – operativer Nutzen und tatsächliche Grenzen

Mit dem biometrischen Internetabgleich wird darüber hinaus ein Instrument geschaffen, das insbesondere für die Identifizierung von Personen sowie die Aufklärung komplexer Tat- und Täterzusammenhänge von erheblicher Bedeutung ist.

Die gesetzliche Ausgestaltung stellt klar, dass es sich um eine einzelfallbezogene Maßnahme handelt, die auf öffentlich zugängliche Daten beschränkt ist und keine Echtzeitanwendungen umfasst. Damit wird der Charakter als zielgerichtetes Ermittlungsinstrument deutlich herausgestellt. Gleichzeitig zeigen sich bei der praktischen Umsetzung erhebliche strukturelle und technische Grenzen.

Ein eigenständiger umfassender Abgleich mit öffentlich zugänglichen Internetdaten ist durch staatliche Stellen aufgrund der Größe und Dynamik der verfügbaren Datenräume faktisch nicht realisierbar. Der Aufbau eigener Referenzdatenbanken würde erhebliche rechtliche und tatsächliche Probleme aufwerfen und zwangsläufig große Datenmengen unbeteiligter Personen erfassen. Eine solche Lösung ist weder realistisch noch politisch gewollt. In der praktischen Konsequenz wird der biometrische Internetabgleich daher vor allem in besonders gewichtigen Fallkonstellationen Anwendung finden, insbesondere im Bereich der Terrorismusabwehr sowie der schweren und organisierten Kriminalität, während ein Einsatz im Bereich mittlerer Kriminalität regelmäßig ausscheidet.

4. Digitale Souveränität und operative Realität

Besonders deutlich wird an dieser Stelle das Spannungsfeld zwischen dem berechtigten politischen Ziel digitaler Souveränität und der operativen Realität der Sicherheitsbehörden. Die Gesetzentwürfe sind bewusst technikoffen formuliert und ermöglichen den Rückgriff auf externe Anbieter.

Diese Offenheit ist aus Sicht der kriminalpolizeilichen Praxis derzeit unverzichtbar, da leistungsfähige Systeme für großskalige biometrische Abgleiche aktuell nicht in einer Form innerhalb Europas verfügbar sind, die den Anforderungen der Praxis gerecht wird. Die effektive Durchführung eines solchen Abgleichs setzt den Zugriff auf bereits strukturierte und umfangreiche Referenzdatenbestände voraus, die gegenwärtig überwiegend von privaten Anbietern bereitgestellt werden.

Die praktische Relevanz dieser Entwicklung ist zuletzt im Zusammenhang mit der Festnahme der ehemaligen RAF-Terroristin Daniela Klette deutlich geworden. Ermittlungsansätze im Zusammenhang mit öffentlich zugänglichen Bilddaten wurden hierbei maßgeblich unter Nutzung kommerzieller Systeme generiert, auf die staatliche Stellen bislang nur eingeschränkt zugreifen können. Vergleichbare Anwendungen werden derzeit insbesondere von Anbietern wie PimEyes oder Clearview AI bereitgestellt, während gleichwertige europäische Lösungen nach unserem Kenntnisstand bislang nicht in vergleichbarer Breite verfügbar sind.

Eine Beschränkung auf ausschließlich europäische Technologien würde unter den aktuellen Rahmenbedingungen dazu führen, dass die Befugnis in wesentlichen Einsatzbereichen faktisch nicht genutzt werden kann. Digitale Souveränität ist daher als strategisches Ziel zu begreifen, nicht als kurzfristige Einsatzvoraussetzung. Der Aufbau eigener oder europäischer Systeme ist notwendig und muss konsequent vorangetrieben werden. Gleichzeitig darf dies nicht dazu führen, dass bereits heute verfügbare und für die Gefahrenabwehr und Kriminalitätsbekämpfung erforderliche Fähigkeiten eingeschränkt werden.

5. Einsatz außereuropäischer Technologien und praktische Umsetzung

Die im Gesetzentwurf vorgesehene Möglichkeit, biometrische Abgleiche unter Einbindung von Stellen außerhalb der Europäischen Union durchzuführen, trägt dieser Realität Rechnung und ist für die praktische Nutzbarkeit der Befugnis von zentraler Bedeutung. Zugleich entstehen hierdurch erhöhte Anforderungen an die rechtliche und tatsächliche Kontrolle der Datenverarbeitung. In der praktischen Umsetzung wird die Nutzung entsprechender Systeme regelmäßig über polizeiliche oder justizielle Rechtshilfewege erfolgen müssen, was zusätzliche Verfahrensschritte und zeitliche Verzögerungen mit sich bringt. Dies gewinnt insbesondere in dynamischen Einsatzlagen an Bedeutung, in denen schnelle Entscheidungen erforderlich sind.

6. Richtervorbehalt, Bürokratie und zeitkritische Einsatzrealität

Vor diesem Hintergrund ist auch der vorgesehene Richtervorbehalt für Maßnahmen unter Einbindung von Drittstaaten zu betrachten. Dieser ist grundsätzlich geeignet, eine zusätzliche rechtsstaatliche Kontrolle sicherzustellen und die besondere Eingriffsqualität der Maßnahme angemessen zu flankieren.

In der praktischen Anwendung ist jedoch zu berücksichtigen, dass der biometrische Internetabgleich typischerweise in zeitkritischen Einsatzlagen erfolgt. Gerade in Situationen, in denen eine schnelle Identifizierung oder Lokalisierung erforderlich ist, besteht regelmäßig ein erheblicher Zeitdruck. Die Möglichkeit der Anordnung bei Gefahr im Verzug trägt diesem Umstand Rechnung, führt jedoch dazu, dass der Richtervorbehalt in Eilkonstellationen häufig nachgelagert zur Anwendung kommt.

Im Zusammenhang mit dem vorgesehenen Richtervorbehalt stellt sich daher die Frage, wie die praktische Ausgestaltung des Kontrollmechanismus so erfolgen kann, dass sowohl eine wirksame rechtsstaatliche Kontrolle gewährleistet als auch den Anforderungen zeitkritischer Einsatzlagen ausreichend Rechnung getragen wird. Der zusätzliche Verfahrensschritt kann in der Praxis mit einem erhöhten administrativen Aufwand verbunden sein, weshalb es darauf ankommt, die Abläufe möglichst effizient und praxistauglich zu gestalten.

Ziel sollte es sein, Kontrollmechanismen so auszugestalten, dass sie sowohl rechtsstaatlich wirksam als auch operativ handhabbar sind und insbesondere in zeitkritischen Einsatzlagen eine zügige Durchführung der Maßnahmen unterstützen.

7. Technische Umsetzung, Programm Polizei 2020 und strukturelle Voraussetzungen

Die Wirksamkeit der vorgesehenen Regelungen hängt entscheidend von ihrer praktischen Umsetzbarkeit ab. Neue Befugnisse entfalten nur dann Wirkung, wenn sie auf einer leistungsfähigen technischen Infrastruktur aufsetzen. Hier zeigt sich ein zentrales strukturelles Defizit der deutschen Sicherheitsarchitektur. Trotz langjähriger Initiativen wie dem Programm Polizei 2020 und der damit verbundenen Zielsetzung einer bundeseinheitlichen, interoperablen IT-Landschaft bestehen weiterhin erhebliche Unterschiede zwischen Bund und Ländern sowie zwischen einzelnen Behörden.

Gerade im Bereich der Analyse- und Auswertungssysteme ist bislang keine durchgängig einheitliche und leistungsfähige Struktur entstanden. Datenbestände sind häufig nicht kompatibel, Systeme nicht miteinander verknüpft und Auswertungsmöglichkeiten unterschiedlich ausgeprägt. Dies führt dazu, dass vorhandene Informationen nicht vollständig genutzt werden können und erhebliche Erkenntnispotenziale ungenutzt bleiben.

Vor dem Hintergrund der nun vorgesehenen gesetzlichen Erweiterung digitaler Ermittlungsbefugnisse tritt dieses Defizit besonders deutlich hervor. Die neuen Befugnisse setzen zwingend voraus, dass Daten aus unterschiedlichen Quellen zusammengeführt und in einheitlichen Systemen ausgewertet werden können. Ohne eine konsequente Weiterentwicklung und Vereinheitlichung der IT-Strukturen im Rahmen von Polizei 2020 besteht die Gefahr, dass die gesetzlich geschaffenen Möglichkeiten in der Praxis nur eingeschränkt wirksam werden.

Nach mittlerweile rund zehn Jahren seit der Saarbrücker Agenda bedarf es daher einer deutlich konsequenteren Umsetzung der ursprünglich formulierten Ziele. Die Harmonisierung der IT-Landschaft ist keine technische Detailfrage, sondern eine zentrale Voraussetzung für die Funktionsfähigkeit moderner Ermittlungsarbeit.

8. Testen und Trainieren von IT-Systemen

Die vorgesehene Befugnis zum Testen und Trainieren von IT-Systemen ist ausdrücklich zu begrüßen. Sie stellt eine notwendige Voraussetzung für die Entwicklung, den Betrieb und die Qualitätssicherung moderner Analyse- und Auswertungssysteme dar. Ohne die Möglichkeit, Systeme unter realitätsnahen Bedingungen zu entwickeln und zu validieren, wird eine effektive Nutzung der neu geschaffenen Befugnisse nicht möglich sein.

9. Gesamtbewertung und Schlussfolgerung

Die vorliegenden Gesetzentwürfe stellen einen wichtigen und notwendigen Schritt zur Modernisierung der kriminalpolizeilichen Befugnisse dar. Sie tragen den veränderten Rahmenbedingungen der Sicherheitslage Rechnung und schaffen die Grundlage für eine effektivere Nutzung

vorhandener Daten. Gleichzeitig wird deutlich, dass der Erfolg dieser Regelungen nicht allein von ihrer rechtlichen Ausgestaltung abhängt, sondern maßgeblich von der Verzahnung mit technischen, organisatorischen und strategischen Rahmenbedingungen.

Die entscheidende Frage moderner Sicherheitsarchitektur ist nicht mehr, ob Daten vorhanden sind, sondern ob der Staat in der Lage ist, diese rechtssicher, effizient und in einem konsistenten System zu nutzen. Daran wird sich die Wirksamkeit der vorliegenden Reform messen lassen.

Mit freundlichen Grüßen



Dirk Peglow
Bundsvorsitzender