VERBAND DER INTERNETWIRTSCHAFT E.V.

Stellungnahme

zum Referentenentwurf des Bundesministeriums des Innern für ein Gesetz zur Stärkung digitaler Ermittlungsbefugnisse zur Abwehr von Gefahren des internationalen Terrorismus

Berlin, 02.04.2026

Mit dem Referentenentwurf will das Bundesministerium des Innern dem Bundeskriminalamt zusätzliche digitale Ermittlungsbefugnisse für die Abwehr von Gefahren des internationalen Terrorismus einräumen. Der Entwurf begründet dies mit einer angespannten Sicherheitslage, insbesondere durch internationalen Terrorismus, schwere Gewalttaten und eine wachsende Bedrohung durch organisierte und gewaltbereite Strukturen. Ziel des Gesetzes ist es nach der Begründung, den Polizeibehörden die rechtlichen Instrumente zur Verfügung zu stellen, um diesen Herausforderungen wirksamer zu begegnen.

Inhaltlich steht in diesem Entwurf der automatisierte biometrische Abgleich mit öffentlich zugänglichen Daten aus dem Internet im Zentrum. Nach der Begründung soll er insbesondere dazu dienen, Personen zu identifizieren, zu lokalisieren und Zusammenhänge zwischen Personen, Strukturen und Taten aufzudecken. Zugleich verweist die Begründung ausdrücklich darauf, dass bei der Ausübung der Befugnis auch eine Zusammenarbeit mit Dritten, einschließlich Stellen außerhalb der Europäischen Union, möglich sein soll. Aus Sicht des eco ist gerade diese Befugnis hochproblematisch. Auch im Bereich der Terrorismusabwehr rechtfertigt der Sicherheitszweck nicht die Einführung einer weitreichenden gesetzlichen Grundlage für biometrische Internetrecherchen. Vor diesem Hintergrund adressieren wir nachfolgend die aus unserer Sicht zentralen Punkte.

1. Vorgesehene gesetzliche Änderungen

Der Entwurf beschränkt sich auf eine Änderung des Gesetzes über das Bundeskriminalamt (BKAG) und führt dort zwei neue Befugnisse ein. § 39a BKAG-E sieht nun den automatisierten biometrischen Abgleich mit öffentlich zugänglichen Daten aus dem Internet und § 39b BKAG-E die automatisierte Datenanalyse vor. Beide Befugnisse sind auf die Aufgabe des Bundeskriminalamts zur Abwehr von Gefahren des internationalen Terrorismus zugeschnitten.

Gemeinsamer Kern der Neuregelungen ist, dass das Bundeskriminalamt vorhandene Datenbestände technisch erheblich weitergehend verarbeiten darf als bisher. Zum einen soll es biometrische Merkmale, insbesondere Lichtbilder, mit öffentlich zugänglichen Daten aus dem Internet automatisiert abgleichen dürfen, um Personen zu identifizieren, ihren Aufenthaltsort zu ermitteln oder Zusammenhänge zwischen Straftaten und Strukturen aufzudecken. Zum anderen soll das BKA Daten, auf die es zur Aufgabenerfüllung zugreifen darf, automatisiert zusammenführen und analysieren können, um Beziehungen, Muster und Verknüpfungen zwischen Personen, Vorgängen, Organisationen und Objekten sichtbar zu machen.

2. Bewertung des eco

eco lehnt die Einführung des automatisierten biometrischen Abgleichs mit öffentlich zugänglichen Daten aus dem Internet ab.

Trotz des spezifischen Terrorismusbezugs bleibt die vorgesehene Maßnahme eine besonders eingriffsintensive Form staatlicher Datenverarbeitung. Der Ausschluss von Echtzeitdaten ändert nichts daran, dass das frei zugängliche Internet systematisch als biometrischer Suchraum erschlossen werden soll. Der Entwurf nennt selbst als Zweck Identifizierung, Aufenthaltsermittlung und Zusammenhangsermittlung. Damit geht es gerade nicht nur um punktuelle Ermittlungsunterstützung, sondern um eine technische Verdichtung verstreuter personenbezogener Informationen zu einem neuen Erkenntnisbild.

Der Verweis auf den Terrorismusbezug als Rechtfertigung überzeugt nicht ohne Weiteres. Gerade weil die Abwehr terroristischer Gefahren einen besonders sensiblen und hoch aufgeladenen Bereich betrifft, bedarf es engster tatbestandlicher Begrenzungen, starker Verfahrensgarantien und wirksamer Kontrolle. Der Entwurf schafft jedoch eine Befugnis, die zwar formell an besonders gewichtige Gefahrenlagen anknüpft, materiell aber weitreichende biometrische Such- und Analyseoperationen im Internet ermöglicht. Aus Sicht des eco besteht hier die Gefahr, dass ein außergewöhnliches Instrument rechtlich verstetigt und technisch normalisiert wird.

Davon abgesehen bestehen erhebliche Risiken für Fehlidentifikationen, Diskriminierung und unverhältnismäßige Betroffenheit Unbeteiligter. Biometrische Systeme sind nicht neutral. Biometrische Erkennung muss strengen Schutzvorkehrungen unterliegen. Aus Sicht des eco ist daher biometrische Überwachung im öffentlichen Raum besonders kritisch zu bewerten ist. Biometrische Erkennung darf, wenn überhaupt, nur in eng begrenzten Einzelfällen und unter starken Sicherungen in Betracht kommen. Diese Linie gilt erst recht, wenn nicht nur der öffentliche Raum, sondern praktisch das gesamte frei zugängliche Internet als Datenquelle erschlossen werden soll.

Besonders problematisch ist die Möglichkeit, den biometrischen Abgleich durch öffentliche oder nichtöffentliche Stellen durchführen zu lassen. Der Entwurf ist ausdrücklich technik- und produktneutral ausgestaltet und eröffnet damit die Nutzung externer technischer Lösungen. Noch gravierender ist, dass bei Vorliegen zusätzlicher Voraussetzungen sogar Übermittlungen an Stellen in Drittstaaten vorgesehen sind. Gerade bei biometrischen Daten drohen hier Kontrollverluste, Zweckentfremdung und erhebliche datenschutzrechtliche Risiken. Dass ein Richtervorbehalt nur für Drittstaatenkonstellationen vorgesehen ist, während die Einschaltung Dritter im Inland oder in der EU ohne vergleichbare Hürde möglich bleibt, ist aus rechtsstaatlicher Sicht nicht überzeugend.

Die vorgesehenen Schutzmechanismen können ebenso nicht überzeugen. Löschungs- und Protokollierungspflichten sind wichtig, beseitigen aber nicht das strukturelle Problem des Grundrechtseingriffs. Dieser liegt bereits in der automatisierten biometrischen Durchsuchung des frei zugänglichen Netzes. Hinzu kommt, dass der Entwurf auf eine Befristung und Evaluierung verzichtet. Für eine neue und besonders eingriffsintensive Befugnis im Bereich der Terrorismusabwehr ist das ein erhebliches Defizit.

Der Entwurf überschreitet mit dem automatisierten biometrischen Abgleich öffentlich zugänglicher Internetdaten eine kritische Schwelle. Er beschränkt sich zwar institutionell auf das Bundeskriminalamt und sachlich auf die Abwehr von Gefahren des internationalen Terrorismus. Gerade in diesem besonders sensiblen Bereich müssten die rechtsstaatlichen Sicherungen jedoch

besonders stark ausgeprägt sein. Das ist nicht der Fall. Stattdessen schafft der Entwurf eine neue gesetzliche Grundlage für weitreichende biometrische Internetrecherchen, erlaubt die Einschaltung externer Stellen und verzichtet zugleich auf Befristung und Evaluierung.

Aus Sicht des eco ist dieser Ansatz abzulehnen. Sicherheitspolitische Ziele dürfen nicht dazu führen, dass biometrische Fernidentifizierung und umfassende digitale Verknüpfungsbefugnisse im Namen der Terrorismusabwehr schrittweise zum Regelfall werden. Erforderlich sind klare rechtsstaatliche Grenzen, starke Schutzmechanismen und eine offene gesellschaftliche Debatte. Genau daran fehlt es dem Entwurf in seiner jetzigen Fassung.
