VERBAND DER INTERNETWIRTSCHAFT E.V.

**Stellungnahme**

**zum Referentenentwurf des Bundesministeriums des Innern für ein Gesetz zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit**

Berlin, 02.04.2026

Mit dem Referentenentwurf will das Bundesministerium des Innern Bundeskriminalamt, Bundespolizei und im Asylbereich das Bundesamt für Migration und Flüchtlinge mit zusätzlichen digitalen Ermittlungsbefugnissen ausstatten. Nach der Begründung des Entwurfs sollen die Behörden dadurch auf eine verschärfte Sicherheitslage, insbesondere im Bereich Terrorismus sowie schwere und organisierte Kriminalität, reagieren können. Zentraler Baustein des Entwurfs ist neben der automatisierten Datenanalyse vor allem der biometrische Abgleich mit öffentlich zugänglichen Daten aus dem Internet. Der Entwurf selbst benennt als Ziel insbesondere die Identifizierung und Lokalisierung von Personen sowie die Ermittlung von Tat-Täter-Zusammenhängen. Zugleich soll eine Zusammenarbeit mit Dritten, auch außerhalb der Europäischen Union, ermöglicht werden.

Aus Sicht des eco ist gerade dieser biometrische Internetabgleich hochproblematisch. Er greift tief in grundrechtlich geschützte Freiheitsräume ein, birgt erhebliche Risiken für Fehlidentifikationen, Profilbildung und Diskriminierung und ist in seiner Reichweite weiter, als es die Begründung des Entwurfs zunächst erkennen lässt. Bereits in der Debatte um das Sicherheitspaket 2024 hat eco deshalb betont, dass neue Kompetenzen für Sicherheitsbehörden nur dann überhaupt diskutiert werden können, wenn sie mit präzisen Schutzmaßnahmen, klaren gesetzlichen Grenzen und einer breiten gesellschaftlichen Debatte einhergehen. Vor diesem Hintergrund adressieren wir nachfolgend die aus unserer Sicht zentralen Punkte.

## 1. Vorgesehene gesetzliche Änderungen

Der Referentenentwurf schafft im Gesetz über das Bundeskriminalamt (BKAG) und im Bundespolizeigesetz (BPolG) jeweils neue Befugnisse für den automatisierten biometrischen Abgleich mit öffentlich zugänglichen Daten aus dem Internet und passt die bereits bestehende Regelung im Asylgesetz inhaltlich daran an. Gemeinsamer Kern aller Änderungen ist, dass staatliche Stellen biometrische Daten, insbesondere Lichtbilder, mit im Internet frei zugänglichen personenbezogenen Daten automatisiert abgleichen dürfen sollen, um Personen zu identifizieren, ihren Aufenthaltsort zu ermitteln oder Zusammenhänge zwischen Personen, Sachverhalten, Straftaten und Gefahrenlagen aufzudecken.

Die vorgesehenen Regelungen folgen dabei einem einheitlichen Muster. Sie erlauben die Erhebung öffentlich zugänglicher Internetdaten mit biometrischen Merkmalen, deren automatisierten Abgleich mit bereits vorhandenen behördlichen Datenbeständen sowie die weitere Verarbeitung von Treffern für den jeweiligen Ermittlungs- oder Gefahrenabwehrzweck. Ausgenommen sein sollen lediglich öffentlich zugängliche Echtzeitdaten. Zugleich sieht der Entwurf Löschungs-, Protokollierungs- und einzelne Datenschutzvorgaben vor.

Besonders relevant ist, dass die Maßnahmen nicht auf klassische Beschuldigtensachverhalte beschränkt bleiben. Je nach Regelungsbereich können sie auch im präventiven Gefahrenabwehrkontext, zur Aufenthaltsermittlung oder gegenüber weiteren betroffenen Personen eingesetzt werden. Hinzu kommt, dass der biometrische Abgleich nicht zwingend durch die Behörde selbst erfolgen muss. Der Entwurf erlaubt vielmehr auch die Einschaltung öffentlicher oder nichtöffentlicher Stellen im Inland und in anderen EU-Mitgliedstaaten, teilweise ist sogar eine Durchführung durch Stellen in Drittstaaten vorgesehen.

## 2. Bewertung des eco

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

Der Entwurf schafft eine Befugnis, die weit über punktuelle Fahndungsmaßnahmen hinausgeht. Auch wenn der Abgleich mit Echtzeitdaten ausgeschlossen wird, bleibt es bei einer äußerst eingriffsintensiven Form biometrischer Fernidentifizierung. Die technische Durchsuchung öffentlich verfügbarer Bilder und Videos im Internet erlaubt Rückschlüsse auf Identität, Aufenthaltsorte, Kontakte und Verhaltensmuster. Der Entwurf selbst nennt ausdrücklich Identifizierung, Lokalisierung und die Ermittlung von Zusammenhängen als Ziel. Damit besteht das reale Risiko einer verdichteten digitalen Profilbildung.

Außerdem bleibt der Begriff der „öffentlich zugänglichen Daten aus dem Internet“ zu unbestimmt. Schon früher hat eco hervorgehoben, dass gerade an dieser Stelle besondere Vorsicht geboten ist. Wenn unklar bleibt, welche Inhalte erfasst werden dürfen, entsteht die Gefahr, dass Daten aus Graubereichen, halböffentlichen Räumen oder kontextgebundenen Veröffentlichungen faktisch in biometrische Suchläufe einbezogen werden. eco hält es für rechtsstaatlich nicht hinnehmbar, eine so weitreichende Eingriffsbefugnis auf einen Begriff zu stützen, dessen praktische Konturen unscharf bleiben. Genau hier hatte eco bereits im Zusammenhang mit dem Sicherheitspaket präzise gesetzliche Grenzen und Schutzmaßnahmen gefordert.

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 an dem Entwurf ist, dass der Anwendungsbereich nicht auf Beschuldigte beschränkt bleibt. Im BKA-Bereich können unter bestimmten Voraussetzungen auch Zeugen, Opfer, Kontaktpersonen und Auskunftspersonen betroffen sein. Im Bundespolizeibereich können Nichtverantwortliche einbezogen werden, soweit überwiegende schutzwürdige Interessen nicht entgegenstehen. Im Asylbereich trifft die Regelung zudem eine besonders vulnerable Personengruppe. Damit verschiebt der Entwurf die Maßnahme von einem Instrument gegen konkret Verdächtige hin zu einer Befugnis, die auch das Umfeld und teilweise unbeteiligte Personen erfasst.

Die nach dem Entwurf vorgesehene Einschaltung öffentlicher und nichtöffentlicher Stellen verschärft die Risiken erheblich. Der Entwurf ist ausdrücklich technik- und produktneutral. Die Begründung nennt sogar die Nutzung kommerzieller Produkte Dritter. Damit wird die Tür für sensible

biometrische Verarbeitung durch externe Anbieter geöffnet. Hinzu kommt, dass in bestimmten Fällen sogar eine Übermittlung an Drittstaaten vorgesehen ist. Gerade bei biometrischen Daten sind Zweckentfremdung, Kontrollverluste und Missbrauchsrisiken besonders gravierend. Dass hierfür im inländischen und unionsinternen Bereich keine vergleichbar strengen Hürden wie bei Drittstaaten vorgesehen sind, ist nicht überzeugend.

Die vorgesehenen Schutzmechanismen können ebenso nicht überzeugen. Dass Echtzeitdaten ausgeschlossen, einzelne Löschungspflichten normiert und Protokollierungspflichten vorgesehen sind, beseitigt die strukturellen Probleme der Maßnahme nicht. Der eigentliche Grundrechtseingriff liegt bereits in der automatisierten biometrischen Durchsuchung des frei zugänglichen Netzes. Hinzu kommt, dass der Entwurf weder eine Befristung noch eine Evaluierung vorsieht. Für eine derart neue und eingriffsintensive Befugnis ist das ein erhebliches Defizit.

Insgesamt steht der Entwurf für einen problematischen Regulierungsansatz. Wo der Staat tief in digitale Freiheitsräume eingreift, ist gesellschaftliches Vertrauen in Technologie besonders wichtig. eco hat hierzu bereits hervorgehoben, dass weitreichende biometrische Befugnisse nicht das Vertrauen in KI und digitale Technologien stärken, sondern eher gefährden, wenn sie ohne hinreichende Debatte und ohne präzise Schutzmaßnahmen vorangetrieben werden.

---