VERBAND DER INTERNETWIRTSCHAFT E.V.

Stellungnahme

zum Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz für ein Gesetz zur Änderung der Strafprozessordnung – digitale Ermittlungsmaßnahmen

Berlin, 02.04.2026

Mit dem Referentenentwurf will das Bundesministerium der Justiz und für Verbraucherschutz die Strafverfolgungsbehörden mit neuen digitalen Ermittlungsbefugnissen ausstatten, um die Effektivität der Strafverfolgung zu steigern. Der Entwurf benennt hierfür zwei Regelungsschwerpunkte. Zunächst soll eine ausdrückliche Rechtsgrundlage für den automatisierten biometrischen Abgleich von Daten aus einem Strafverfahren mit im Internet öffentlich zugänglichen Daten geschaffen werden. Darüber hinaus sollen die Strafverfolgungsbehörden befugt werden, verfahrensübergreifende Recherche- und Analyseplattformen einzusetzen. Zur Begründung verweist der Entwurf insbesondere auf fehlende ausdrückliche Ermächtigungsgrundlagen, steigende Datenmengen, Effizienzdefizite manueller Ermittlungsarbeit sowie auf Anforderungen aus der KI-Verordnung der EU und der Rechtsprechung des Bundesverfassungsgerichts zur automatisierten Datenanalyse.

Der Entwurf schafft damit neue strafprozessuale Grundlagen für besonders eingriffsintensive Formen staatlicher Datenverarbeitung. Das betrifft vor allem den biometrischen Internetabgleich, aber auch die verfahrensübergreifende Auswertung großer, bereits in Polizeisystemen zusammengeführter Datenbestände. Aus Sicht des eco wirft der Entwurf deshalb erhebliche rechtsstaatliche, datenschutzrechtliche und grundrechtliche Fragen auf. Vor diesem Hintergrund adressieren wir nachfolgend die aus unserer Sicht zentralen Punkte.

1. Biometrischer Internetabgleich in der StPO als neuer, besonders eingriffsintensiver Standardzugriff

Mit § 98d StPO-E würde der automatisierte biometrische Abgleich erstmals ausdrücklich in das strafprozessuale Ermittlungsinstrumentarium aufgenommen. Damit würde eine hochsensible Form biometrischer Fernidentifizierung nicht mehr nur randständig, sondern systematisch im Strafverfahren verankert. Zwar verweist der Entwurf darauf, dass bislang manuelle OSINT-Maßnahmen möglich seien. Der entscheidende Unterschied liegt aber gerade in der Automatisierung. Der Entwurf selbst erkennt an, dass dadurch potentiell viele Unbeteiligte betroffen sein können und dass die Maßnahme in das Recht auf informationelle Selbstbestimmung eingreift.

Aus Sicht des eco ist diese Entwicklung abzulehnen. Der automatisierte biometrische Abgleich erlaubt es, Bilder, Videos oder andere biometrische Referenzdaten aus einem Strafverfahren gegen große Mengen öffentlich zugänglicher Internetdaten laufen zu lassen. Damit wird das Internet faktisch zu einem staatlichen Such- und Identifizierungsraum. Der Eingriff liegt nicht erst im Treffer, sondern bereits in der Erfassung, dem automatisierten Vergleich und der weiteren Auswertung der Daten. Daran ändert auch der Ausschluss von Echtzeitdaten nichts.

Hinzu kommt, dass der Entwurf den Begriff der „öffentlich zugänglichen Daten“ sehr weit versteht. Erfasst sein sollen nicht nur frei erreichbare Inhalte, sondern ausdrücklich auch Daten, die nach

vorheriger Registrierung, Genehmigung oder Entgeltzahlung genutzt werden können. Nicht erfasst seien lediglich Daten aus klar begrenzten, kontrollierten Zugangsbereichen oder Privatkommunikation über Messenger-Dienste. Diese Auslegung ist aus Sicht des eco deutlich zu weit. Sie eröffnet die Gefahr, dass auch kontextgebunden veröffentlichte oder nur formal „öffentliche“ Inhalte in biometrische Suchläufe einbezogen werden.

Besonders problematisch ist zudem, dass die Maßnahme nicht nur gegenüber Beschuldigten, sondern ausdrücklich auch gegenüber Zeugen eingesetzt werden kann. Damit wird ein Instrument von erheblicher Eingriffsintensität über die klassische Beschuldigtenstellung hinaus erweitert. Dies verschiebt die strafprozessuale Balance erheblich. Aus Sicht des eco ist es rechtsstaatlich nicht überzeugend, biometrische Internetrecherchen auch gegenüber Personen zu eröffnen, die nicht Beschuldigte sind.

2. Vorgesehene Schutzmechanismen nicht ausreichend

Der Entwurf enthält zwar einzelne Sicherungen wie den Ausschluss von Echtzeitdaten, Löschungs- und Protokollierungspflichten, eine staatsanwaltschaftliche Anordnung sowie die Einbeziehung von Benachrichtigungspflichten über § 101 StPO. Außerdem verweist die Begründung auf flankierende Vorgaben aus der KI-Verordnung und dem Datenschutzrecht. Diese Sicherungen ändern aber nichts daran, dass der Gesetzgeber hier eine neue und strukturell weitreichende Eingriffsbefugnis schafft.

Aus Sicht des eco fällt besonders ins Gewicht, dass kein Richtervorbehalt vorgesehen ist. Die Maßnahme soll grundsätzlich durch die Staatsanwaltschaft angeordnet werden. Bei Gefahr im Verzug sogar zunächst durch Ermittlungspersonen. Für eine Ermittlungsmaßnahme, die biometrische Fernidentifizierung mit Internetrecherchen verbindet, ist das nicht ausreichend. Wenn biometrische Erkennung überhaupt in Betracht gezogen wird, bedarf sie jedenfalls starker Schutzvorkehrungen. eco hat bereits im AI-Act-Kontext hervorgehoben, dass biometrische Erkennung mindestens strengen Sicherungen unterliegen muss, nur in eng begrenzten Einzelfällen eingesetzt werden sollte und einer besonders hohen grundrechtlichen Sensibilität unterliegt.

3. Verfahrensübergreifende Datenanalyse schafft ein neues Niveau polizeilicher Verknüpfungsbefugnisse im Strafverfahren

Noch weiterreichender ist § 98e StPO-E. Die Norm erlaubt nicht nur einen punktuellen Abgleich, sondern eine systematische, verfahrensübergreifende Analyse zusammengeführter Polizeidatenbestände. Der Entwurf will hierfür ausdrücklich an bereits vorhandene Analyseplattformen der Gefahrenabwehr anknüpfen. Damit würde eine Infrastruktur, die für präventive Zwecke geschaffen wurde oder geschaffen werden soll, nun auch repressiv für die Strafverfolgung nutzbar gemacht. Genau darin liegt aus Sicht des eco ein zentraler Problempunkt. Die Trennlinien zwischen Gefahrenabwehr und Strafverfolgung werden weiter aufgeweicht, während gleichzeitig die technische Fähigkeit wächst, aus heterogenen Datenbeständen komplexe Personen-, Beziehungs- und Lagebilder zu erzeugen.

Der Entwurf beschreibt selbst sehr deutlich, wie weit die Methode reicht. Er erlaubt die Identifikation und Herstellung von Beziehungen und Zusammenhängen zwischen Personen, Gruppen, Institutionen, Organisationen, Verfahren, Vorgängen, Objekten und Sachen, ihre qualitative und quantitative Klassifizierung, ihre strukturelle Analyse und Visualisierung sowie statistische Auswertungen. Damit geht die Befugnis weit über einen klassischen Datenabgleich hinaus. Auch wenn der Entwurf betont, es solle keine automatisierte Einzelfallentscheidung geben und der Mensch müsse am Anfang und Ende des Entscheidungsprozesses stehen, bleibt die Maßnahme hoch eingriffsintensiv. Sie ist gerade

darauf angelegt, aus verstreuten Datenbeständen neues Wissen, neue Verdachtsmomente und neue Ermittlungsansätze zu generieren.

Besonders bedenklich ist, welche Daten in diese Systeme einbezogen werden können. Neben Vorgangs- und Falldaten sowie Daten aus polizeilichen Informationssystemen und dem polizeilichen Informationsaustausch können unter Voraussetzungen auch Daten aus anderen Verfahren einfließen, darunter Telekommunikationsdaten, Standortdaten, Daten aus Funkzellenabfragen, Inhaltsdaten aus Telefonüberwachung und Daten aus Asservaten. Zwar werden Daten aus Online-Durchsuchung und Wohnraumüberwachung anderer Verfahren ausgenommen. Das ändert jedoch nichts daran, dass die Norm eine breit angelegte Zusammenführung und Weiterverarbeitung hochsensibler Bestände ermöglicht. Das Risiko umfassender Profilbildung ist erheblich.

4. Flankierende Verweise auf KI-Verordnung und Datenschutzrecht ersetzen keine materiell enge Befugnisnorm

Der Entwurf verweist mehrfach auf die KI-Verordnung, Datenschutz-Folgenabschätzungen, Bias-Prüfungen, Transparenzpflichten und datenschutzrechtliche Kontrolle. Solche Anforderungen sind wichtig. Sie können aber eine materiell zu weit gefasste Eingriffsbefugnis nicht heilen. Aus Sicht des eco ist es problematisch, technische und organisatorische Anforderungen an Systeme mit der Frage zu vermengen, ob und in welchem Umfang der Staat bestimmte Maßnahmen überhaupt durchführen dürfen soll. Datenschutz-Folgenabschätzung, Dokumentation und Marktüberwachung ersetzen keine enge tatbestandliche Begrenzung, keinen wirksamen Richtervorbehalt und keine klare politische Entscheidung gegen eine Normalisierung biometrischer Fernidentifizierung im Strafverfahren.

5. Fazit

Mit dem Referentenentwurf zur Änderung der Strafprozessordnung würde der Gesetzgeber zwei neue digitale Ermittlungsinstrumente in das Strafverfahren einführen, die in ihrer Kombination besonders weit reichen. Beide Instrumente versprechen aus Sicht des Entwurfs mehr Effizienz. Tatsächlich schaffen sie jedoch neue, tiefgreifende Eingriffsbefugnisse mit erheblichem Missbrauchs-, Fehler- und Ausweitungsrisiko.

Strafverfolgung in einer digitalen Gesellschaft darf nicht dazu führen, dass biometrische Fernidentifizierung und umfassende Plattformanalysen schrittweise zum neuen Standard werden. Erforderlich sind klare rechtsstaatliche Grenzen, materielle Eingriffsschranken, unabhängige Kontrolle und eine offene Debatte über die Frage, welche Formen automatisierter Identifizierung und Datenverknüpfung in einem freiheitlichen Rechtsstaat überhaupt zulässig sein sollen.

Über eco: Mit rund 1.000 Mitgliedsunternehmen ist eco (www.eco.de) der führende Verband der Internetwirtschaft in Europa. Seit 1995 gestaltet eco maßgeblich das Internet, fördert neue Technologien, schafft Rahmenbedingungen und vertritt die Interessen seiner Mitglieder gegenüber der Politik und in internationalen Gremien. eco hat Standorte in Köln, Berlin und Brüssel. eco setzt sich in seiner Arbeit vorrangig für ein leistungsfähiges, zuverlässiges und vertrauenswürdiges Ökosystem digitaler Infrastrukturen und Dienste ein.