GESELLSCHAFT
FÜR INFORMATIK

Berlin, 10. Dezember 2025

Stellungnahme

der Gesellschaft für Informatik e.V. (GI)

zu den Entwürfen der Bundesregierung zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit

Stand: Referentenentwürfe vom 26.6.2025

Am 24.7.2025 sind zwei Referentenentwürfe des Bundesministeriums des Inneren zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit öffentlich bekannt geworden. Das Bundeskabinett strebt zu diesem Zweck die Verabschiedung zweier Kabinettsentwürfe im Oktober 2025 an.

Das Gesetzespaket ist in zwei Teile aufgeteilt: In dem ersten Gesetz sind die zustimmungsfreien Bestandteile des Pakets enthalten. Für das zweite Gesetz ist die Zustimmung des Bundesrates notwendig. Mit diesen Entwürfen sollen die Befugnisse des Bundeskriminalamtes und der Bundespolizei erweitert werden. Mit der Erweiterung des Asylgesetzes (AsylG) macht die Bundesregierung darüber hinaus die Identifizierung mittels biometrischen Abgleichs bei Asylsuchenden möglich.

Die Gesellschaft für Informatik e.V. (GI) positioniert sich mit dieser Stellungnahme klar gegen die beiden Gesetzesentwürfe.

Grundsätzliche Einschätzung

Die Entwürfe des Bundesministeriums des Innern vom 26. Juni 2025 sehen u.a. die anlasslose biometrische Gesichtserkennung im Internet, den Einsatz kommerzieller Software zur Auswertung von Gesichts- bzw. Verhaltensdaten (z.B. Clearview, PimEyes, Palantir) sowie die Zusammenführung und automatisierte Auswertung großer Datenbestände durch Polizeibehörden vor.

Aus fachlicher Sicht bestehen gravierende Bedenken hinsichtlich der technischen Machbarkeit, IT-Sicherheitsrisiken, der Vereinbarkeit mit dem Datenschutz sowie der Gewährleistung rechtsstaatlicher Kontrollmechanismen. Selbst wenn die in den Referentenentwürfen vorgesehenen Maßnahmen tatsächlich umsetzbar und rechtmäßig wären, würden sie dennoch ihr eigentliches Ziel verfehlen: Sie können nach fachlicher Einschätzung der GI weder die erforderliche Qualität und Verlässlichkeit der Analyseergebnisse erreichen, noch können sie einen wirksamen Beitrag und Mehrwert zur Ermittlungsarbeit leisten.

Die GI lehnt biometrische Überwachungsverfahren zur Gesichtserkennung im öffentlichen Raum ab und fordert die Bundesregierung auf, die Gesetzesentwürfe nicht ins parlamentarische Verfahren einzubringen. Den im Referentenentwurf geplanten Einsatz von automatisierter Datenanalyse, dem biometrischen Internetabgleich, sowie dem Testen und Trainieren von IT-Produkten inkl. selbstlernenden Systemen (ugs. KI-Systeme) bewertet die GI sehr kritisch. Die GI schließt sich anderen zivilgesellschaftlichen Organisationen in ihrer Ablehnung des Gesetzesvorhabens ausdrücklich an.

Im Einzelnen

1. Datenerfassung aus dem Internet und Datenspeicherung

Biometrische Daten sind hochsensible persönliche Informationen über körperliche Eigenschaften und Verhaltensweisen wie Gesichtsausdruck und Mimik, Gestik und Bewegungsmuster oder Stimmen. Dazu gehört beispielsweise auch, wie Menschen mit ihren Augen ein Bild erfassen. Der Referentenentwurf des BMI umfasst sämtliche Möglichkeiten der Erfassung biometrischer Daten. Mithilfe digitaler Werkzeuge sollen

biometrische Daten mit im Internet öffentlich zugänglichen Daten und Bildersuchmaschinen abgeglichen und für Ermittlungsverfahren oder zur Identifizierung von Asylsuchenden eingesetzt werden.

Ein biometrischer Datenabgleich ist nur möglich, wenn eine Datenbank zum Abgleich von Individuen für alle Personen, im Einzelfall anlasslos gespeichert, bereits existiert. Laut Art. 5 Abs. 1 KI-Verordnung ist das ungezielte Sammeln von Gesichtsbildern im Sinne des Aufbaus einer „Superdatenbank" sowie die biometrische Echtzeit-Fernidentifizierung ausdrücklich verboten[1]. Erwägungsgrund 43 spezifiziert weiter, dass die Begründung des Verbots besonders im „Gefühl der Massenüberwachung" sowie in der Verletzung des Rechts auf Privatsphäre liegt.[2] Aus fachlicher Sicht ist die beliebige Zusammenführung und Verarbeitung von Daten sowie auch nach den allgemeinen Datenschutzregelungen (u.a. JI-RL, DSGVO, BKAG und BDSG) die anlasslose Speicherung dieser, etwa von Verkehrs- und Standortdaten[3], unzulässig. **Eine solche Datenerfassung und -speicherung ist aus fachlicher Sicht deshalb klar abzulehnen.**

2. **Verarbeitung von Daten inkl. personenbezogenen Daten zum Zwecke des Trainings von Analysesystemen und für die automatisierte Datenanalyse**

Der Entwurf sieht weiterhin vor, dass automatische Analysesysteme inkl. selbstlernende Systeme mit personenbezogenen, nicht anonymisierten Daten trainiert und getestet werden dürfen. Dieser Einsatz widerspricht grundlegenden Datenschutzprinzipien[4]. Zudem bleibt ungeklärt, auf welcher neu zu schaffenden, spezialgesetzlichen Rechtsgrundlage die Nutzung solcher personenbezogener (nichtanonymisierter) Daten erfolgen soll.

Problematisch ist aus Sicht der GI die geplante Verarbeitung in großen Datenbanken mithilfe von automatisierter Datenanalyse. Automatische Gesichts- und Verhaltenserkennung sind sehr fehleranfällig sowie häufig diskriminierend und stellen daher einen schweren Eingriff in unsere Grundrechte dar. Die Einschätzung des Bundesverfassungsgerichts, dass automatisierte Datenanalysen verfassungswidrig sind[5], hält die GI weiterhin für richtungsweisend.

Es bleibt außerdem unklar, wozu die Analysesysteme konkret eingesetzt werden sollen. Wenn diese versuchen, aus einzelnen Datenpunkten über eine Person statistische Zusammenhänge zu konstruieren, die in Wirklichkeit nicht existieren oder die nicht kausal nachvollziehbar sind, kann das technisch weder zuverlässig Kriminalität vorhersagen noch nützliche Hinweise für Ermittlungen liefern. Ein Grund dafür ist, dass Straftaten oft sehr unterschiedlich verlaufen und deshalb meist als Einzelfälle kontextspezifisch betrachtet werden müssen. **Aus Sicht der GI ist das Trainieren und Testen von Analysesystemen mit personenbezogenen Daten deshalb abzulehnen.**

---

[1] https://www.europarl.europa.eu/topics/de/article/20230601STO93804/ki-gesetz-erste-regulierung-der-kunstlichen-intelligenz

[2] https://www.bundesnetzagentur.de/DE/Fachthemen/Digitales/KI/8_VerbotenePraktiken/start.html sowie *https://artificialintelligenceact.eu/de/recital/43/*

[3] Wir verweisen hier auf die Stellungnahme der GI zur Vorratsdatenspeicherung: https://gi.de/fileadmin/GI/user_upload/GI-Stellungnahme_Quick_Freeze.pdf

[4] vgl. Art. 5 DSGVO https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016R0679

[5] https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2023/02/rs20230216_1bvr154719.html

3. Abgleich sämtlicher biometrischer Daten aus dem Internet

Die vorgesehenen Befugnisse ermöglichen einen generellen Abgleich öffentlich zugänglicher Bilder im Internet. Dies entspricht technisch einer permanenten Rasterfahndung und führt zwangsläufig zu hohen Fehlerraten (False Positives), insbesondere bei heterogenen Bildquellen[6] oder sehr ähnlichen Bildmotiven (z.B. Zwillingen, Familienmitgliedern), was zu unrechtmäßigen Verdächtigungen führen kann.

Der biometrische Abgleich mit öffentlich zugänglichen Daten schließt zwar im Begründungstext private Chats sowie geschlossene Gruppen und ähnliches aus. Es ist jedoch nicht auszuschließen, dass verwendete trainierte Modelle, insbesondere große Sprachmodelle, auch mit privat verfügbaren Daten trainiert wurden und daher solche Daten indirekt Einfluss auf Analyseprozesse haben.

Zudem bleibt die Frage der Verlässlichkeit von Daten für einen Abgleich, d.h. die Datenauthentizität, aus öffentlich zugänglichen Quellen im Internet völlig offen: Es ist heutzutage für viele Personengruppen möglich, beliebige Daten (z.B. Fotos, Videos, Texte) schnell und massenhaft im Internet zu veröffentlichen und geeignet zu verbreiten (z.B. in Social Media). So können insbesondere Fehlinformationen, darunter auch gezielt manipulierte oder künstlich erzeugte Inhalte über andere Personen (z.B. deren Aufenthaltsort, deren Aussagen, gefälschte oder künstlich generierte Fotos, etc.) massenhaft gestreut werden. Die Unterscheidung zwischen authentischen und verfälschten Daten ist technisch nicht durchführbar und stellt auch für Menschen eine erhebliche Herausforderung dar.

Vor diesem Hintergrund ist fraglich, welchen Nutzen automatisierte Abgleiche mit Daten aus dem Internet überhaupt haben können, wenn die Echtheit bzw. Authentizität der Daten nicht gesichert werden kann. Statt eines Mehrwertes entsteht hier vielmehr ein Schadwert: Personen laufen Gefahr, mit (ggf. gezielt) unauthentischen, bewusst manipulierten oder gefälschten Daten aus dem Internet in Verbindung gebracht zu werden. Die Praxis hybrider Kriegsführung oder digitaler Propaganda, etwa durch massenhafte Verbreitung gezielt ausgerichteter Falschaussagen, Bilder und Videos zur Einflussnahme auf die öffentliche Meinung, zeigen auf, dass dies kein hypothetisches Szenario, sondern bereits Realität ist. **Aus Sicht der GI verfehlt ein Datenabgleich den Nutzen, Ermittlungsarbeit verlässlich zu unterstützen und läuft Gefahr, Personen unrechtmäßig zu verdächtigen. Der Datenabgleich ist aus diesen Gründen abzulehnen.**

4. Fehlende rechtliche Begrenzungen eines Datenabgleichs

Aus Sicht der Informatik sind „Security by Design“ und „Privacy by Design“ anerkannte Standards; gesetzliche Regelungen müssen diese Prinzipien widerspiegeln. Sie sorgen dafür, dass Sicherheits- und Datenschutzaspekte schon bei der Entwicklung von IT-Systemen berücksichtigt werden, anstatt sie nachträglich zu ergänzen. Die Gesetzesentwürfe beinhalten bisher keinerlei rechtliche Hürden und Eingriffsschwellen, wie es bei einer solchen Eingriffsschwere angemessen wäre. Eine Überprüfung der Anwendbarkeit der Überwachung im Einzelfall fehlt im

[6] Grother, Patrick / Ngan, Mei / Hanaoka, Kayee (2025): Face recognition technology evaluation (FRTE). Part 2: Identification. Gaithersburg: National Institute of Standards and Technology (NIST). https://pages.nist.gov/frvt/reports/1N/ frvt_1N_report.pdf (abgerufen am 07.07.2025)

Gesetzesentwurf – eine Sicherheitsvorkehrung, die besonders zum Schutz der personenbezogenen Daten unerlässlich ist. Richtervorbehalte fehlen gänzlich.

Der Einsatz eines automatisierten Datenabgleichs zum Zwecke der Identifikation von Menschen laut Art. 4 Nr. 1 des Referentenentwurfs (aktualisierter § 15b AsylG) sieht keinerlei Beschränkungen vor – selbst eine vorherige Prüfung alternativer Ausweisdokumente und vorherige Ausschöpfung milderer Mittel sind im Entwurf nicht verankert. Im Sinne des im Grundgesetz verbrieften Schutzes der Privatsphäre sind diese genauso auch auf Asylsuchende an der Grenze anzuwenden. Zusätzlich sieht der Entwurf bei Anwendung lediglich eine Überprüfung durch zwei Personen vor, deren Verantwortungsrang, Kompetenz, Ausbildung und Befugnis nicht weiter benannt ist.

Darüber hinaus geht vom zu ändernden § 15b AsylG das erhebliche Risiko aus, dass Herkunftsstaaten über Anträge von Asylsuchenden in Kenntnis gesetzt werden. Technisch kann dies durch den Datenabgleich von Analysesystemen bei den Betreibern der jeweiligen Server sichtbar werden. Zusätzlich kann ein Heimatland über die IP-Adresse, von der aus die Anfrage in der biometrischen Datenbank gestartet wird, auch ungefähre Informationen über den aktuellen Aufenthaltsort schlussfolgern. Zudem weist der Sachverständige Wittmann bei der öffentlichen Anhörung zum Sicherheitspaket 2024 darauf hin, dass es in der technischen Natur von selbstlernenden Systemen liegt, dass eingespeiste Daten für das erneute Training der Algorithmen weitergenutzt werden. Aus diesem Grund nehmen laut Wittmann bspw. auch deutsche Behörden Abstand davon, sicherheitskritische Informationen in KI-Systeme einzuspeisen, die im Ausland betrieben werden[7]**Fehler! Textmarke nicht definiert.**.

Des Weiteren ermöglichen § 10b und §10c BKAG einen nachträglichen biometrischen Abgleich mit Internetdaten sowie eine automatisierte Datenanalyse bereits bei geplanten oder tatsächlichen Straftaten im Sinne des § 100a Abs. 2 StPO – eine niedrige Schwelle angesichts der geplanten Eingriffsschwere. Zudem sind im Entwurf eine Dokumentation der Behörden, u.a. des BAMF über den Umfang, Zweck und Notwendigkeit der Nutzung des biometrischen Abgleichs mit Internetdaten, Transparenz über die Überwachungstätigkeit gegenüber den Betroffenen, sowie effektive Rechtsmittel für eine Überprüfung bzw. Klage gänzlich zu vermissen. Die GI plädiert daher dafür, „Security by Design“ und „Privacy by Design“ in Gesetzesentwürfen zentral zu verankern und im Falle eines Abgleichs hohe rechtliche Eingriffsschwellen, Kontrollmechanismen und Rechtsschutz für Betroffene zu verankern.

5. Geplanter Einsatz von kommerziellen Software-Anbietern, auch außerhalb der Europäischen Union

Den Umgang mit personenbezogenen Daten in der Europäischen Union regelt die DSGVO. Der Einsatz proprietärer Plattformen außerhalb der Europäischen Union wie Palantir, die europäischen verfassungskonformen und rechtsstaatlichen Standards nicht entsprechen und mit autoritären Regimen zusammenarbeiten, gefährdet die Nachvollziehbarkeit, Prüfbarkeit, Kontrollierbarkeit und langfristige Integrität der Systeme. Aus Sicht der GI müsste der Gesetzesentwurf mindestens eine Weitergabe von personenbezogenen Daten an Dritte (§ 22 Abs. 3 BKAG) außerhalb der

[7] https://www.bundestag.de/resource/blob/1019538/20-4-493-A-neu.pdf

Europäischen Union oder des Schengen-Raums ausdrücklich ausschließen. Zudem muss davon ausgegangen werden, dass die zu großen Teilen personenbezogenen Daten von US-Unternehmen wie bspw. Palantir gemäß US Cloud Act u.a. an US-Behörden weitergegeben werden. Biometrische Daten zählen als besonders schützenswerte Daten, gerade für vulnerable Gruppen. Dies beinhaltet auch Menschen, die nach Art. 16a GG als politisch Verfolgte Asylrecht[8] genießen und deren Daten aufgrund der eigenen Verfolgung oder ggf. in Rücksichtnahme auf Familienangehörigen im Herkunftsland besonders schützenswert sind, auch im digitalen Raum. **Die GI fordert aus diesen Gründen den konsequenten Ausschluss des Einsatzes von kommerziellen Software-Anbietern.**

6. Gefahren für die IT-Sicherheit

Die explizite Ermöglichung der bisherigen Referentenentwürfe einer Zusammenarbeit mit Dritten, auch außerhalb der Europäischen Union ohne jegliche weitere Spezifizierung und Begrenzung schafft eine unvergleichbar größere Angriffsfläche für Angriffe auf die IT-Sicherheit der Ermittlungsbehörden. Das Zusammenführen großer Datensätze zum Zwecke des Aufbaus einer zentralen Datenbank für das Ziel des biometrischen Datenabgleichs widerspricht dem Grundsatz der Datenminimierung und hebt die Zweckbindung erfasster Daten auf.[9] Dies erhöht die Angriffsfläche für Cyberkriminalität, Datenabfluss, Manipulation und Missbrauch erheblich. **Eine Zusammenarbeit und Datenweitergabe mit Dritten ohne Zweckbindung und Begrenzung des Zugriffs ist aus Sicht der GI auszuschließen.**

7. Verlässlichkeit von Analysesystemen als Policy-Lösung

Zum aktuellen Stand ist es nach Auffassung der GI nicht möglich, dass ein trainiertes Modell die Arbeit von Ermittlungsbehörden anlassbezogen in einem Einzelfall verlässlich ergänzen kann. Es kann nicht davon ausgegangen werden, dass trainierte Modelle verlässlich korrekte Informationen ausgeben, auf die sich Strafverfolgungsbehörden stützen können. Die GI verweist hier auf ihre Stellungnahme zum Umgang mit personenbezogenen Daten in KI-Modellen im Rahmen einer Konsultation der BfDI[10]: Wenn ein Modell auf der Grundlage der Trainingsdaten eine Frage nach einer Person nicht beantworten kann, gibt es die wahrscheinlichste Antwort. Das heißt, es erstellt beispielsweise ein fiktives, typisches Persönlichkeitsprofil, das gegebenenfalls falsch oder durch Klischees verfälscht ist. Die Ausgabe solcher inferierter Informationen nennt man Halluzination. Das trainierte Modell selbst kann zwischen Memorisierung und Halluzination nicht unterscheiden und könnte keine Auskunft darüber geben, welcher Teil des Profils aus gespeicherten Daten stammt und welcher Teil erfunden ist. **Aus diesen dargelegten Gründen warnt die GI davor, trainierte Modelle einschließlich selbstlernender Systeme als vermeintliche „technische Lösungen“ für Aufgaben und Einschätzungen der Ermittlungsbehörden zu nutzen.**

8. Grundrechtliche Risiken

[8] https://www.gesetze-im-internet.de/gg/art_16a.html
[9] https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Stellungnahmen/2021/Positionspapier_Zweckbindung-Polizei.pdf?__blob=publicationFile&v=1 (S. 6)
[10] https://gi.de/meldung/gi-beantwortet-fragen-der-datenschutzbeauftragten-zu-llms

Datenanalysen, die z.B. auf Techniken des maschinellen Lernens oder auf selbstlernenden Systemen aufbauen, bergen die Gefahr von Bias und Diskriminierung. Technisch muss davon ausgegangen werden, dass Minderheiten und marginalisierte Gruppen überproportional falsch erfasst oder belastet werden. Diverse Studien konnten etwa nachweisen, dass Analysesysteme insbesondere bei vulnerablen Gruppen und Frauen überproportional viele Fehlklassifikationen liefern. Dies trifft aufgrund von verzerrten Trainingssätzen ebenso Kinder, ältere Menschen und People of Colour[11].

Die untersuchten Effekte bei vergangenen Einsätzen von Polizeien und Gerichten in den USA sind hier einschlägige Negativbeispiele: So zeigen Studien, dass urbane, eher von Schwarzen Menschen bewohnte Distrikte immer intensiver von Patrouillen überwacht werden[12] und dass die Risiko-Einschätzungen durch das COMPAS-System, ein Algorithmus zur Schätzung des Rückfallrisikos von Straftätern, mit einer höheren Wahrscheinlichkeit Schwarzen Menschen eine zukünftige Straftat zuschreibt[13]. **Aus fachlicher Sicht warnt die GI daher vor den gravierenden grundrechtlichen Risiken, die mit dem Einsatz von trainingsbasierten Datenanalysen für die Strafverfolgung einhergeht.**

9. Einführung von Evaluationspflichten

Ein effektives Monitoring ist zwingend geboten, um die Zweckmäßigkeit der Regierungsentwürfe zu prüfen. Dieses sollte sowohl eine vorausgehende Analyse zur Notwendigkeit, Wirksamkeit und Effizienz der erweiterten Befugnisse, sowie eine gesetzliche Evaluierungspflicht beinhalten. Der Mangel einer solchen Evaluation wurde vom Bundesrechnungshof bereits bei der Ratifizierung der NIS2-Regulierung moniert[14]. Die Evaluierung muss insbesondere die Effizienz und Effektivität des Gesetzes feststellen und sollte darum auf einem fest vorgeschriebenen Zeitpunkt sowie im Vorhinein festgelegten, messbaren Kriterien beruhen. **Aus Sicht der GI sollte dem Gesetzespaket zwingend eine Analyse zur Wirksamkeit und Notwendigkeit vorausgehen und eine Evaluation verpflichtend verankert werden.**

Fazit

Die vorliegenden Entwürfe des Bundesinnenministeriums sind aus Sicht der GI nicht nachbesserungsfähig. Sie beruhen auf Konzepten massenhafter, anlassloser Datensammlung und Überwachung, setzen auf Zusammenarbeit mit Technologien, die nach europäischem Recht nicht zulässig sind und missachten grundlegende Prinzipien

[11] Grother, Patrick / Ngan, Mei / Hanaoka, Kayee (2019): Face recognition vendor test (FRVT). Part 3: Demographic effects. Gaithersburg: National Institute of Standards and Technology (NIST). https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf (abgerufen am 21.08.2025)

[12] Ensign et al., 2018: https://proceedings.mlr.press/v81/ensign18a.html

[13] Angwin et al., 2016: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

[14] Bericht nach § 88 Absatz 2 BHO zum Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung, Ausschussdrucksache 21(4)049 (2025). https://gruen-digital.de/wp-content/uploads/2025/09/214049_-_BRH_-_Bericht_NIS-2-Richtlinie_-_geschwaerzt.pdf.

von IT-Sicherheit, Datenschutz und rechtsstaatlicher Kontrolle. Das Gesetz beruht auf Annahmen in Bezug auf aktuelle Softwaresysteme zur Datenanalyse (Korrektheit, Nutzen, Verlässlichkeit), die so aktuell nicht zutreffen. Die geplante Zentralisierung sensibler Daten, fehlende Eingriffsschwellen und der Verzicht auf einen klaren Anlassbezug führen zu einer technischen Scheinlösung, die IT-Systeme in der Konsequenz unsicherer macht, Grundrechte massiv einschränkt und im Widerspruch zu deutschem und EU-Recht steht.

Als Gesellschaft für Informatik e.V. lehnen wir die Entwürfe daher in ihrer Gesamtheit ab. Wir fordern das Bundesinnenministerium auf, die aktuellen Entwürfe zurückzuziehen und in einem transparenten Verfahren gemeinsam mit Wissenschaft, Zivilgesellschaft und Fachöffentlichkeit einen neuen, grundrechtskonformen und technisch verantwortbaren Entwurf zu erarbeiten.

Über die Gesellschaft für Informatik e.V. (GI)

Die Gesellschaft für Informatik e.V. (GI) ist die größte Fachgesellschaft für Informatik im deutschsprachigen Raum. Seit 1969 vertritt sie die Interessen der Informatikerinnen und Informatiker in Wissenschaft, Gesellschaft und Politik und setzt sich für eine gemeinwohlorientierte Digitalisierung ein. Mit 14 Fachbereichen, über 30 aktiven Regionalgruppen und unzähligen Fachgruppen ist die GI Plattform und Sprachrohr für alle Disziplinen in der Informatik. Weitere Informationen finden Sie unter www.gi.de.