AG KRITIS

Arbeitsgruppe Kritische Infrastrukturen

Stellungnahme zum Ref-E des Bundesministeriums des Innern (BMI) für ein Gesetz zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit

im Rahmen der Verbändebeteiligung

Version 1.0 – zuletzt editiert am 02.04.2026

Inhaltsverzeichnis

1 Arbeitsgruppe Kritische Infrastrukturen

Dieses Dokument wurde von Mitgliedern der unabhängigen Arbeitsgruppe Kritische Infrastrukturen (AG KRITIS) erstellt.

Wir haben uns im Frühjahr 2018 erstmals zusammengefunden, um Ideen und Anregungen zur Erhöhung der Resilienz und Sicherheit kritischer Dienstleistungen von Betreibern kritischer Infrastrukturen im Sinne des Gemeinwohls zu entwickeln. Unser Ziel ist es, die Versorgungssicherheit der deutschen Bevölkerung zu erhöhen, indem wir die Bewältigungskapazitäten des Staates zur Bewältigung von Großschadenslagen, die durch Cyberangriffe hervorgerufen wurden, ergänzen und erweitern wollen. Unsere Arbeitsgruppe ist unabhängig von Staat, Verwaltung oder wirtschaftlichen Interessen.

Die AG KRITIS besteht aus ca. 23 Fachleuten und Experten, die sich mit Kritischen Infrastrukturen (KRITIS) beruflich beschäftigen, zum Beispiel durch Planung, Aufbau, Betrieb sowie Beratung, Forschung oder Prüfung der beteiligten Systeme und Anlagen.
Unser Engagement ist getrieben von der Motivation, unabhängig von wirtschaftlichen Interessen eine nachhaltige Verbesserung der Sicherheit jener Anlagen kooperativ mit allen Beteiligten herbeizuführen und damit im Katastrophenfall die öffentliche Sicherheit zu verbessern. Wir sind kein Wirtschaftsverband oder Unternehmen und haben daher auch und insbesondere keine Sponsoren.

Uns eint, dass wir durch unsere Arbeit unabhängig voneinander zu dem Schluss gekommen sind, dass die Ressourcen der Bundesrepublik Deutschland zur Bewältigung von Großschadenslagen auf Grund von informations- und operationstechnischen Vorfällen im Bereich der Kritischen Infrastrukturen nicht ausreichen. In der Folge sind resultierende Krisen oder Katastrophen nicht oder kaum zu bewältigen. Es sollen daher Wege gefunden werden, das Eintreten gravierender Folgen dieser Vorfälle durch schnelles und kompetentes Handeln zu verhindern oder zumindest abzuschwächen und eine Regelversorgung in kürzest möglicher Zeit wieder sicherzustellen.

2 Stellungnahme

Gefahr des Überwachungsstaats

Die digitale Öffentlichkeit, insbesondere Social-Media-Plattformen, werden zu einer ständig verfügbaren Ermittlungsressource der Sicherheitsbehörden. Wer sich dort zeigt, muss damit rechnen, algorithmisch identifiziert und in komplexe Analyseprozesse einbezogen zu werden.

Damit verschiebt sich das Verhältnis zwischen Staat und Bürgerinnen und Bürgern weiter in Richtung einer vorsorglichen, datengetriebenen Beobachtungslogik. Aus rechtsstaatlicher Sicht verstärkt dies das Risiko einer Normalisierung digitaler Überwachung.

Der Entwurf greift tief in das Recht auf informationelle Selbstbestimmung ein und verstärkt Tendenzen hin zu einer umfassenderen digitalen Überwachungsarchitektur.

Die Kombination aus biometrischem Internetabgleich, umfassender automatisierter Datenanalyse und KI-Trainingsbefugnissen macht die digitale Öffentlichkeit faktisch zu einer permanenten Ermittlungsressource: Wer sich online zeigt, muss damit rechnen, algorithmisch erkannt und in komplexe Analysen einbezogen zu werden, was das Verhältnis zwischen Bürger und Staat in Richtung eines Überwachungsstaats mit generalisiertem Misstrauen und ständiger potenzieller Beobachtung verschiebt.

Auch wenn der Entwurf formal an schwere Delikte, gewichtige Rechtsgüter und bestimmte Aufgabenbereiche anknüpft, besteht das Risiko eines Function Creep: Einmal geschaffene technische und rechtliche Infrastrukturen können später auf weitere Deliktsbereiche, Behördenkontexte oder niedrigere Eingriffsschwellen ausgeweitet werden.

Der Referentenentwurf des BMI zielt darauf ab, die digitalen Befugnisse der Polizei weitreichend im Bereich der Gefahrenabwehr und Strafverfolgung auszuweiten. Dies betrifft den automatisierten biometrischen Abgleich mit öffentlich zugänglichen Internetdaten, die automatisierte Datenanalyse und das Testen und Trainieren von IT-Produkten, einschließlich selbstlernender (KI-)Systeme.

„Von hervorgehobener Bedeutung sind die Befugnisse im Rahmen der Aufgabe des Bundeskriminalamts als Zentralstelle.“ Die Gesetzesänderungen betreffen damit nicht nur vordergründig Bundeskriminalamt und die Bundespolizei, sondern sind über die BKA-Zentralstellenfunktion auch relevant für alle anderen Polizeien in den Ländern (Stichworte hier auch: P20 und das Datenhaus).

Die neuen Befugnisse greifen insbesondere in das Recht auf informationelle Selbstbestimmung, in Datenschutzrechte und in das allgemeine Persönlichkeitsrecht ein. Der Entwurf rechtfertigt dies mit einer hohen abstrakten Bedrohungslage durch internationalen Terrorismus sowie durch schwere und organisierte Kriminalität – dabei hinterlassen einige Sätze aber auch den Eindruck:

Wenn es zu aufwendig erscheint, kommt eben neue (KI-)Technik zum Einsatz, weil es so dann eben für die Polizei „zweckmäßiger“ ist. Was ist das für eine Begründung in einer Demokratie? Der Zweck heiligt nicht alle Mittel.

2.1 Automatisierte Datenanalyse

2.1.1 Etablierung einer weitreichenden Infrastruktur automatisierter Datenanalyse

Die neuen §§ 9b und 63c BKAG sowie § 58b BPolG schaffen weitreichende Befugnisse zur automatisierten Datenanalyse und knüpfen dabei ausdrücklich an die Rechtsprechung des Bundesverfassungsgerichts vom 16. Februar 2023 an.

Das BVerfG hat bereits festgestellt, dass die automatisierte Datenanalyse eine besondere Eingriffsintensität besitzt.

Obwohl der Entwurf betont, dass keine neuen Daten erhoben, sondern nur vorhandene Daten mittels einer automatisierten Anwendung zusammengeführt und zu Analysezwecken weiterverarbeitet und ausgewertet werden, bleibt die Erzeugung „neuen Wissens“ durch automatisierte Datenanalyse verfassungsrechtlich besonders sensibel. Gerade die algorithmische Verknüpfung bereits vorhandener Daten kann Erkenntnisse hervorbringen, die weit über den Aussagegehalt der einzelnen Ausgangsdaten hinausgehen.

Die Begründung stellt klar, dass die Zusammenführung der relevanten Datenbestände technisch „vom Einzelfall und weiteren Eingriffsschwellen unabhängig“ vorgehalten werden soll, um eine schnelle Analyse zu ermöglichen. Außerdem hänge die konkrete Ausgestaltung „von der technischen Lösung ab“. Da bleibt sehr viel offen, wie das in der Praxis dann umgesetzt wird.

Die Begründung geht technisch ersichtlich von einem bereits zusammengeführten und aktualisierten Grunddatenbestand aus, der für spätere Analysen vorgehalten wird. Damit wird eine Infrastruktur geschaffen, in der Daten schon vor der konkreten Einzelanalyse in auswertbarer Form zusammengeführt werden. Das erhöht das Risiko verfahrensübergreifender Mustererkennung und eines späteren Funktionswandels hin zu breiteren, weniger anlassbezogenen Datenanalysen.

Fraglich ist zudem, ob die vorgesehene personelle Schulung und menschliche Kontrolle ausreichen, um diskriminierende oder verzerrte algorithmische Ergebnisse rechtzeitig zu erkennen und in der Praxis wirksam zu korrigieren.

2.1.2 Eine Frage der Auslegung der Zukunft dank Prognosespielräumen

§ 9b Absatz 1 BKAG unterscheidet zwischen repressiver und präventiver Nutzung: Für die Strafverfolgung ist ein Verdacht auf eine Straftat aus dem Katalog des § 100a Absatz 2 StPO

erforderlich, die „auch im Einzelfall schwer wiegt“ – was bedeutet dieses schwer wiegen genau?

Präventiv wird eine konkretisierte Gefahrenlage für eine Straftat aus demselben Katalog gefordert, die sich gegen besonders gewichtige Rechtsgüter (Bestand oder Sicherheit des Bundes/Landes, Leib, Leben oder Freiheit, bedeutende Sachwerte) richtet. Die Begründung verweist ausführlich auf die Rechtsprechung des Bundesverfassungsgerichts, wonach automatisierte Datenanalyse nur bei hinreichend konkretisierten Gefahren für besonders gewichtige Rechtsgüter zulässig sei und daher ein enger Deliktskatalog gerechtfertigt sei.

Im Bereich der Bundespolizei (§ 58b BPolG) wird der Anwendungsbereich darüber hinaus auf Straftaten im Zusammenhang mit lebensgefährdenden Schleusungen sowie Straftaten gegen die Sicherheit des Bahn-, Luft- oder Seeverkehrs erstreckt, wobei bereits eine „nicht unerhebliche Schädigung“ der genannten Rechtsgüter ausreichen soll. Der Begriff der „nicht unerheblichen Schädigung“ ist ebenfalls unbestimmt.

Gerade wegen der besonderen Eingriffsintensität verlangt die Rechtsprechung des Bundesverfassungsgerichts eine strenge Begrenzung automatisierter Datenanalyse auf hinreichend konkretisierte Gefahrenlagen und besonders gewichtige Rechtsgüter. Vor diesem Hintergrund sind unbestimmte Begriffe wie „schwer wiegt“ oder „nicht unerhebliche Schädigung“ rechtspolitisch und verfassungsrechtlich besonders problematisch.

2.1.3 Datenquellenausweitung und Profilbildungsrisiken

Obwohl eine direkte Anbindung an Register außerhalb der Richtlinie (EU) 2016/680 und an Internetdienste unzulässig sein soll, eröffnet die Möglichkeit, extern erhobene Register- und Internetdaten gezielt in die Analyse einzuspeisen, faktisch eine vernetzte Auswertung unterschiedlicher Datenräume.

Die Vorschriften erlauben ausdrücklich die einzelfallbezogene Einbeziehung von Datensätzen aus gezielten, auch automatisierten Abfragen in sonstigen staatlichen Registern sowie im Einzelfall erhobener Datensätze aus Internetquellen in die automatisierte Analyse. Damit können – vorbehaltlich der jeweiligen Spezialbefugnisse – Registerdaten, Internetinhalte und polizeiliche Informationssysteme in einer Analysearchitektur zusammengeführt werden, die Beziehungen zwischen Personen, Organisationen, Objekten und Verfahren datei- und systemübergreifend identifiziert, klassifiziert, strukturell analysiert und visualisiert. Die Normen erlauben auch statistische Auswertungen und die Gewichtung von Suchkriterien nach Sachnähe, Aktualität und Erheblichkeit.

Damit wächst das Risiko, dass aus vielen für sich genommen begrenzten Teilinformationen aussagekräftige Persönlichkeits-, Beziehungs- und Verhaltensprofile entstehen, die weit über den Aussagegehalt der einzelnen Ausgangsdaten hinausgehen und entspricht genau dem vom Bundesverfassungsgericht beschriebenen Gefährdungspotential der neuen Wissensproduktion durch Datenanalyse,

(BVerfG Urteil vom 16. Februar 2023: „Indessen liegt ein Grundrechtseingriff hier nicht nur in der weiteren, zusammenführenden Verwendung vormals getrennter Daten, sondern darüber hinaus in der Erlangung besonders grundrechtsrelevanten neuen Wissens, das durch die automatisierte Datenanalyse oder -auswertung geschaffen werden kann,

https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2023/02/rs20230216_1bvr154719.html)

Wer wann was oder wen genau durch das System analysieren lassen darf, entscheidet das BKA. Die Anordnung der Maßnahme wird beim BKA der Präsidentin/dem Präsidenten oder Bediensteten mit Befähigung zum Richteramt übertragen; eine externe richterliche Kontrolle ist – anders als bei besonders eingriffsintensiven Überwachungsmaßnahmen – nicht vorgesehen.

Der Entwurf enthält für die automatisierte Datenanalyse keine spezifische Benachrichtigungspflicht der Betroffenen und keinen besonderen, eigenständigen Rechtsschutzmechanismus. Rechtsschutz dürfte daher im Wesentlichen nur über allgemeine datenschutz- und verwaltungsrechtliche Wege möglich sein, was angesichts der Heimlichkeit und technischen Komplexität der Maßnahme praktisch erschwert ist.

Und auch hier bleibt die Frage: wer schützt den Bürger vor Rechtsfolgen, die aufgrund falscher algorithmischer Ergebnisse getroffen werden?

„Eine ausschließlich auf der Maßnahme nach Absatz 1 beruhende automatisierte Entscheidungsfindung, die unmittelbar eine nachteilige Rechtsfolge für die betroffene Person hat oder diese erheblich beeinträchtigt, ist unzulässig.“

Dieses Verbot klingt gut, aber schützt nicht vor einem „faktischen Automatismus“, wenn menschliche Entscheider die algorithmischen Ergebnisse in der Praxis weitgehend übernehmen.

2.2 Biometrischer Internetabgleich

Die biometrische Suche im Internet wird als neues Ermittlungsinstrument zur Identifizierung, Aufenthaltsermittlung und Zusammenhangsermittlung etabliert.

Die neuen §§ 9a und 63b BKAG sowie § 58a BPolG erlauben dem BKA und der Bundespolizei, öffentlich zugängliche personenbezogene Daten mit biometrischen Merkmalen aus dem Internet zu erheben und mit vorhandenen Datenbeständen automatisiert biometrisch abzugleichen. Nach der Begründung umfasst dies insbesondere Lichtbilder und Videos aus sozialen Medien und sonstigen frei zugänglichen Internetquellen, sofern diese nicht auf einen kontrollierten, begrenzten Personenkreis beschränkt sind.

Die Vorschriften erlauben explizit die Erhebung und Zwischenspeicherung öffentlich zugänglicher Internetdaten zur Verwendung als Referenzmaterial, auch wenn die abgebildeten Personen keinerlei Bezug zu einer Straftat oder Gefahr aufweisen. Zwar sollen Daten ohne „konkreten Ermittlungsansatz“ nach Durchführung des Abgleichs unverzüglich gelöscht

werden, doch bleibt unklar, wie diese Filterung technisch und organisatorisch zuverlässig erfolgen soll, insbesondere bei großen Video- und Bildmengen. Die Maßnahme birgt das Risiko, dass große Mengen öffentlich zugänglicher Bild- und Videodaten (darunter auch Aufnahmen unbeteiligter Personen) technisch erfasst, zwischengespeichert und biometrisch ausgewertet werden.

Wenn früher Kulissenpersonen für eine Wahlichtbildvorlage oder sequenzielle Lichtbildvorlage benötigt wurden, griff man auf erkennungsdienstliche Bilder von Verdächtigen oder Beschuldigten zurück. Also Material, das von der Polizei offen im Rahmen einer polizeilichen Maßnahme bei der Betroffenen Person erhoben worden und danach in INPOL gespeichert worden war.

Nun aber kann jeder, der in Sozialen Netzwerken sein Gesicht zeigt (oder dessen Gesicht in Sozialen Netzwerken auf Videos/Lichtbildern vorhanden ist), potenziell zum Referenzmaterial staatlicher Fahndungsmaßnahmen werden – ohne dass er/sie je in ein polizeiliches Verfahren involviert war oder von dieser Maßnahme erfährt.

Eine ausdrückliche Benachrichtigungspflicht der betroffenen Personen nach Abschluss der Maßnahme ist im Entwurf für den biometrischen Internetabgleich nicht festgeschrieben, obwohl der Eingriffscharakter der biometrischen Erfassung dem heimlicher Überwachungsmaßnahmen vergleichbar ist.

Man denke an die falsch-positiven Treffer und im Extremfall an die unrechtmäßig inhaftierten „Verdächtigen“, die sich als Unschuldige entpuppten, z. B.

https://www.theguardian.com/us-news/2026/mar/12/tennessee-grandmother-ai-fraud

https://www.washingtonpost.com/business/interactive/2025/police-artificial-intelligence-facial-recognition/

https://www.heise.de/news/Gesichsterkennung-in-Grossbritannien-Unschuldige-zu-Unrecht-verdaechtigt-9733112.html

Und was tut man, um zu verhindern, dass sich der Mensch bei der Polizei oder die Institution zu viel auf die neue Technik verlässt, die bekanntermaßen Fehleranfällig ist?

2.2.1 Maßnahmenausweitung dank Auslegungsermessen

Für den strafverfolgungsbezogenen Einsatz verlangt § 9a Absatz 1 BKAG zwar einen Verdacht auf eine Straftat „von auch im Einzelfall erheblicher Bedeutung“, insbesondere aus dem Katalog des § 100a Absatz 2 StPO, sowie die Erforderlichkeit zur Ergänzung vorhandener Sachverhalte und Subsidiarität gegenüber anderen Mitteln. Zugleich ist der Begriff der „Straftat von auch im Einzelfall erheblicher Bedeutung“ weit und strafrechtsdogmatisch nicht eindeutig konturiert, zumal der Entwurf ausdrücklich darauf hinweist, dass der Straftatenkatalog des § 100a Absatz 2 nur „insbesondere, aber nicht ausschließlich“ erfasst sein soll. Dadurch entsteht

ein erhebliches Auslegungsermessen, das zu einer schleichenden Ausweitung auf immer breitere Deliktgruppen führen kann.

Im präventiven Bereich (§ 9a Absatz 1 Nummer 1 zweiter Halbsatz sowie §§ 63b BKAG, 58a BPolG) genügt jeweils, dass „bestimmte Tatsachen die Annahme rechtfertigen“, eine Person werde innerhalb eines „übersehbaren Zeitraums“ eine der bezeichneten Straftaten begehen. Der Begriff des „übersehbaren Zeitraums“ bleibt völlig unbestimmt; die Rechtfertigungsformel „bestimmte Tatsachen rechtfertigen die Annahme“ ist seit langem als relativ niedrige Eingriffsschwelle kritisiert, die erheblich von der konkreten Prognosepraxis abhängt. Damit wird ein hochintensiver, tief in Persönlichkeitsrechte eingreifender biometrischer Abgleich teilweise schon im Vorfeld konkreter Gefahrenlagen ermöglicht, ohne dass der Entwurf den Prognosemaßstab normativ weiter schärft oder objektive Kriterien vorgibt.

Es fehlen strenge quantitative oder qualitative Begrenzungen (z. B. Beschränkung auf klar umrissene Lagen, räumliche oder zeitliche Begrenzung des Abgleichs, Höchstumfänge der zusammengesammelten Datenpools), die die Gefahr einer schleichenden Normalisierung und Ausdehnung dieser Eingriffsbefugnisse mindern könnten.

Zwar erklärt der Entwurf den Abgleich mit öffentlich zugänglichen Echtzeitdaten für unzulässig. Unklar bleibt jedoch, wie genau „Echtzeit“ technisch und rechtlich abgegrenzt wird und ob nur gering verzögerte Datenströme faktisch ähnlich eingriffsintensive Wirkungen entfalten könnten.

2.2.2 Datenübermittlung in Drittstaaten

Der Entwurf ist eine Aufweichung europäischer Datenschutzstandards zugunsten polizeilicher Zweckmäßigkeit: § 9a Absatz 6 BKAG und § 58a Absatz 6 BPolG erlauben die Übermittlung erforderlicher Daten an Stellen in Drittstaaten, wenn dies „zum Zweck des Schutzes der nationalen Sicherheit erforderlich“ ist, und gestatten ausdrücklich Abweichungen von einzelnen Schutzvorgaben des § 81 BDSG.

Die Polizei (BKA und Bundespolizei) kann den biometrischen Abgleich also an ausländische öffentliche und nichtöffentliche Stellen auslagern, die sogar außerhalb der EU sein können.

Was muss man sich unter der Zusammenarbeit mit Dritten auch außerhalb der EU vorstellen? Wer sind solche Dritte konkret?

Es besteht das Risiko, dass biometrische Daten von in Deutschland lebenden Personen in Sicherheitsarchitekturen von Drittstaaten mit geringeren rechtsstaatlichen und sicherheitsrelevanten Standards gelangen.

2.2.3 Was ist mit der Verhältnismäßigkeit?

Transparenz- und Rechenschaftsmechanismen beschränken sich im Wesentlichen auf Protokollierungspflichten und datenschutzaufsichtliche Kontrolle. Ein Richtervorbehalt ist für

den Regelfall der biometrische Internetrecherche nicht vorgesehen. Die richterliche Anordnungspflicht wird ausschließlich für die besonders sensible Konstellation der Drittstaatenübermittlung nach § 9a Absatz 6 BKAG und § 58a Absatz 6 BPolG vorgesehen, nicht aber für den Kern der Maßnahme selbst. Angesichts der Eingriffsintensität erscheint dies rechtsstaatlich unzureichend.

2.3 Testen und Trainieren von IT-Produkten

Vieles von dem, was die Polizei in ihren polizeilichen Informationssystemen an Daten gespeichert hat (einschließlich hochsensibler Fall-, Kommunikations- und Kontextdaten), kann zu einem allgemeinen Trainings-Rohstoff für IT-Systeme werden und ist nicht mehr primär an den ursprünglichen Erhebungszweck gebunden.

Das Prinzip der Datenminimierung wird nicht eingehalten, wenn nun mit personenbezogenen Daten aus dem Echtsystem das Trainingssystem bzw. IT-Produkte (einschließlich selbstlernender Systeme) entwickelt und trainiert werden dürfen. Es reicht, wenn man also einfach einen „unverhältnismäßigen Aufwand“ für die Anonymisierung oder Pseudonymisierung der Echtdaten erklärt. Da lautet die Frage: Was ist ein „unverhältnismäßiger Aufwand“? Wie definiert man das?

Zwar ist das Trainieren mit Daten aus besonders eingriffsintensiven Maßnahmen nach § 12 Absatz 3 BKAG (z. B. Wohnraumüberwachung, verdeckte Eingriffe in IT-Systeme) ausdrücklich ausgeschlossen, doch betrifft dies nur einen Teil der besonders sensiblen Datenbestände. Andere Daten, aus denen Rückschlüsse auf Gesundheit, politische Überzeugungen, religiöse Zugehörigkeit, sexuelle Orientierung oder besonders schutzwürdige Lebensumstände gezogen werden können, sind nicht explizit ausgeschlossen und können damit für Trainingszwecke genutzt werden. Aus grundrechtlicher Sicht stellt dies eine erhebliche Zweckänderung dar, die die Erwartung der Betroffenen, ihre Daten würden ausschließlich zur konkreten Gefahrenabwehr oder Strafverfolgung genutzt, tiefgreifend enttäuscht. Fraglich ist, ob Bürger, die zum Beispiel als Anzeigende/Opfer/Zeugen einen Kontakt mit der Polizei wegen einem Ereignis hatten, nun mit ihren Daten auch Teil einer Softwareentwicklung werden möchten – gezwungenermaßen, ohne jemals ihre Einwilligung dafür gegeben zu haben?

Darüber hinaus dürfen nach § 22 Absatz 4 BKAG und § 46 Absatz 4 BPolG personenbezogene Daten zu Test- und Trainingszwecken an inländische öffentliche oder nichtöffentliche Stellen sowie an bestimmte Stellen anderer EU-Staaten übermittelt werden, sofern dies zur Aufgabenerfüllung erforderlich ist. Zwar enthält die Norm eine Pflicht zur Geheimhaltungsverpflichtung der Empfänger und zur Zweckbindung auf Test- und Trainingszwecke, doch fehlt es an klaren Vorgaben zur Minimierung, Segmentierung nach Sensitivität oder zur Pflicht, Trainingsdaten nach Abschluss des Projekts zu löschen.

Aus polizeifachlicher Sicht kann die Möglichkeit, IT-Produkte realitätsnah mit Echtdaten zu testen, die Qualität von Systemen verbessern und Fehlalarme reduzieren. Gleichzeitig besteht

die Gefahr, dass technische Dienstleister – etwa Softwarehersteller oder Forschungsinstitutionen – einen tiefen Einblick in reale polizeiliche Daten erhalten und damit neue Angriffsflächen für Datensicherheitsverletzungen entstehen. Der Entwurf verweist zwar auf organisatorische und technische Maßnahmen zum Schutz vor unbefugter Kenntnisnahme, beschreibt aber keine konkrete Governance-Struktur für Auswahl, Auditierung und Überwachung externer Partner.

Die Kombination aus weiten Trainingsbefugnissen, externer Datenweitergabe und fehlender evaluativer Befristung begünstigt eine starke Abhängigkeit der Polizeibehörden von komplexen, häufig proprietären KI-Systemen externer Partner. Dies erschwert im praktischen Betrieb die Nachvollziehbarkeit, wie bestimmte Analyse- und Abgleichsergebnisse zustande kommen, und erzeugt neue Haftungs- und Verantwortlichkeitsfragen, wenn fehlerhafte Modelle zu Grundrechtsverletzungen führen. Wer das System nicht versteht und Ergebnisse nicht nachvollziehen kann, kommt in die Gefahr mit seinen Maßnahmen ungewollt die falschen Personen zu treffen.

2.4 Änderungen im Asylgesetz

§ 15b AsylG-E erlaubt es, das beim BAMF erhobene biometrische Lichtbild von Ausländerinnen und Ausländern ohne gültigen Pass oder Passersatz automatisiert mit öffentlich zugänglichen Internetbildern abzugleichen, um Identität oder Staatsangehörigkeit festzustellen. Für eine besonders vulnerable Gruppe wird damit die digitale Öffentlichkeit zum Gegenstand biometrischer Identitätsprüfung.

Zwar sieht § 15b AsylG-E anders als BKAG und BPolG keine Durchführung durch Drittstaaten vor, sondern nur durch inländische Stellen oder Stellen eines EU-Mitgliedstaats. Gleichwohl wirft auch diese externe Durchführung angesichts komplexer IT-Infrastrukturen die Frage auf, ob der Schutz vor Kenntniserlangung durch Herkunfts- oder Verfolgerstaaten in der Praxis stets zuverlässig gewährleistet werden kann.

2.5 Weitere Anmerkungen

2.5.1 Warum haben keine Interessenvertreter oder Personen außerhalb der Bundesverwaltung an dem Entwurf mitgearbeitet?

Der Entwurf erklärt ausdrücklich, dass keine Interessenvertreterinnen und Interessenvertreter Dritter oder sonstige Personen außerhalb der Bundesverwaltung an seiner Erstellung beteiligt wurden (Exekutiver Fußabdruck). Angesichts der tiefgreifenden Auswirkungen auf Grundrechte, digitale Öffentlichkeit und Zivilgesellschaft ist dies problematisch, weil damit datenschutzrechtliche, menschenrechtliche und technische Expertise aus der Zivilgesellschaft, Wissenschaft und Aufsichtseinrichtungen in der frühesten Phase der Normgestaltung ausgeblendet wurde.

Ob sich dieser Mangel an der Beteiligung durch Stellungnahmen nachholen und abfedern lässt, bleibt fraglich.

2.5.2 Warum ist keine Befristung oder evaluationspflichtige Erprobung dieser weitreichenden neuen Ermittlungs-Instrumente vorgesehen?

Der Entwurf verspricht, durch automatisierte Datenanalyse und biometrischen Internetabgleich Verbindungen zwischen Taten, Personen und Orten schneller zu erkennen, komplexe Ermittlungen in Terrorismus- und OK-Verfahren zu unterstützen und in Anschlagssituationen eine schnellere Gefahrenabwehr zu ermöglichen. Diese Ziele sind aus polizeilicher Sicht nachvollziehbar, insbesondere angesichts wachsender Datenmengen und dem Umstand, dass Kriminalität und Bedrohungslagen nicht vor Landesgrenzen halt machen und es eine heterogene Datenbanklandschaft bei den Polizeien in Bund und Ländern gibt.

Aber in der Begründung ist nicht ausreichend belegt, in welchem Umfang bisherige Instrumente tatsächlich versagen und welche konkreten Mehrwerte die neuen Systeme gegenüber bestehenden Auswertungsmöglichkeiten schaffen. Es fehlen empirische Evaluationsdaten, Pilotstudien oder belastbare Szenarioanalysen, die den behaupteten Nutzen quantifizieren und gegen die absehbaren finanziellen, organisatorischen und grundrechtlichen Kosten abwägen.

Der Entwurf sieht weder eine Befristung der Befugnisse noch eine verpflichtende, unabhängige Evaluierung ihrer Wirksamkeit, Grundrechtsverträglichkeit und gesellschaftlichen Folgen vor.

Aus moralischer Sicht ist es bedenklich, Instrumente mit erheblichem Missbrauchs- und Fehlerrisiko dauerhaft zu etablieren, ohne von vornherein Korrektur- und Rücknahmeoptionen normativ zu verankern. Eine experimentelle, befristete Einführung mit klaren Evaluationskriterien würde dem Prinzip der Verantwortlichkeit für die Folgen staatlichen Handelns besser entsprechen als die hier vorgesehene Dauerlösung.

2.5.3 Was ist mit der Souveränität?

Da die Befugnisse technik- und produktneutral ausgestaltet sind, können sowohl Eigenentwicklungen als auch Produkte Dritter eingesetzt werden.

Das Testen und Trainieren von IT-Produkten mit Echtdaten sowie die Möglichkeit, biometrische Abgleiche von privaten oder ausländischen Stellen durchführen zu lassen, schaffen eine enge Verzahnung mit externen Akteuren.

Dies birgt Risiken in Bezug auf Vendor-Lock-in, Geheimhaltungsinteressen kommerzieller Anbieter (Black-Box-Modelle) und Sicherheitslücken in komplexen Softwarelandschaften. Ohne strenge Anforderungen an Offenlegung, Auditierbarkeit und Interoperabilität können Polizeibehörden faktisch in eine Situation geraten, in der sie Entscheidungen maßgeblich auf

Ergebnisse stützen müssen, deren technische Herleitung sie selbst nicht mehr vollständig verstehen oder kontrollieren.

Der Staat sollte sich in sensiblen Bereichen nicht von externen (ausländischen) Akteuren, die eigene Interessen verfolgen (können), abhängig machen.

3 Fazit und Zusammenfassung

Der Referentenentwurf des BMI zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit stellt einen tiefen und in Teilen verfassungsrechtlich nicht hinreichend gerechtfertigten Eingriff in das Recht auf informationelle Selbstbestimmung, in Datenschutzrechte und in das allgemeine Persönlichkeitsrecht dar. Die Zusammenschau der drei zentralen Regelungskomplexe ergibt das Bild einer digitalen Überwachungsarchitektur, die weit über anlassbezogene Einzelfallermittlung hinausgeht und systematisch eine datengetriebene Beobachtungslogik gegenüber der gesamten Bevölkerung etabliert.

Die im Entwurf verwendeten Eingriffsschwellen sind an entscheidenden Stellen normativ unscharf. Begriffe wie "schwer wiegt", "nicht unerhebliche Schädigung" oder "übersehbarer Zeitraum" eröffnen erhebliche Auslegungsspielräume, die in der Praxis zu einer schleichenden Ausweitung der Befugnisse auf immer breitere Deliktgruppen und niedrigere Gefahrenschwellen führen können. Wir fordern, dass diese unbestimmten Rechtsbegriffe durch normativ klar konturierte, objektiv überprüfbare Kriterien ersetzt werden.

Für den biometrischen Internetabgleich und die automatisierte Datenanalyse fehlt ein Richtervorbehalt als Regelvoraussetzung. Angesichts der vom Bundesverfassungsgericht im Urteil vom 16. Februar 2023 ausdrücklich anerkannten besonderen Eingriffsintensität dieser Maßnahmen ist die interne Anordnungskompetenz durch Behördenleitung rechtsstaatlich unzureichend. Wir fordern einen obligatorischen Richtervorbehalt für beide Maßnahmen, nicht nur für den Sonderfall der Drittstaatenübermittlung.

Betroffene Personen, deren biometrische Daten im Rahmen des Internetabgleichs erhoben, zwischengespeichert und ausgewertet werden, werden im Entwurf nicht benachrichtigt. Dies gilt auch dann, wenn sie keinerlei Bezug zu einer Straftat aufweisen und lediglich als Referenzmaterial gedient haben. Wir fordern eine gesetzlich verankerte Benachrichtigungspflicht nach Abschluss der Maßnahme sowie einen eigenständigen Rechtsschutzmechanismus.

Das im Entwurf vorgesehene Verbot rein automatisierter Entscheidungen mit nachteiligen Rechtsfolgen schützt nicht vor dem faktischen Automatismus, der entsteht, wenn menschliche Entscheidungsträger algorithmische Ergebnisse in der Praxis weitgehend ungeprüft übernehmen. Wir fordern konkrete und überprüfbare Anforderungen an die Qualität der menschlichen Prüfung algorithmischer Ergebnisse sowie klare Haftungsregelungen für den Fall falscher algorithmischer Treffer.

Die Nutzung personenbezogener Echtdaten aus polizeilichen Informationssystemen zum Training selbstlernender IT-Systeme stellt eine erhebliche Zweckentfremdung dar, die dem Grundsatz der Datenminimierung widerspricht. Wir fordern, dass besonders sensible Datenkategorien, insbesondere solche, aus denen Rückschlüsse auf Gesundheit, politische

Überzeugungen, religiöse Zugehörigkeit oder sexuelle Orientierung möglich sind, ausdrücklich vom Trainingseinsatz ausgeschlossen werden.

Der Entwurf enthält weder eine zeitliche Befristung der neuen Befugnisse noch eine Pflicht zur unabhängigen Evaluation ihrer Wirksamkeit und gesellschaftlichen Folgen. Es fehlen empirische Grundlagen, die belegen, dass bestehende Ermittlungsinstrumente tatsächlich versagen und die neuen Systeme einen konkreten, quantifizierbaren Mehrwert schaffen. Wir fordern eine evaluationspflichtige, befristete Erprobungsphase mit klaren Erfolgskriterien und der Option zur normativen Rücknahme, bevor diese Befugnisse dauerhaft etabliert werden.

Schließlich ist es demokratiepolitisch nicht hinnehmbar, dass ein Entwurf mit derart weitreichenden Grundrechtswirkungen ausschließlich innerhalb der Bundesverwaltung erarbeitet wurde. Wir fordern, dass in einem strukturierten Konsultationsverfahren externe Sachverständige aus Datenschutz, Rechtswissenschaft, Technikfolgenabschätzung und zivilgesellschaftlichen Organisationen verbindlich einbezogen werden, bevor der Entwurf das parlamentarische Verfahren erreicht**.**