



# AG KRITIS

Arbeitsgruppe Kritische Infrastrukturen

**Stellungnahme zum Ref-E des  
Bundesministeriums des Innern (BMI)  
für ein Gesetz zur Stärkung digitaler  
Ermittlungsbefugnisse zur Abwehr von  
Gefahren des internationalen  
Terrorismus**

**im Rahmen der Verbändebeteiligung**

## Inhaltsverzeichnis

1 Arbeitsgruppe Kritische Infrastrukturen.....	3
2 Stellungnahme.....	4
2.1 Automatisierter biometrischer Internetabgleich (§ 39a BKAG-E).....	5
2.1.1 Kooperation mit Dritten und Datenübermittlung in Drittstaaten.....	6
2.2 Automatisierte Datenanalyse (§ 39b BKAG-E).....	6
2.2.1 Der Gesetzesentwurf ermöglicht den Aufbau einer dauerhaften Analyseinfrastruktur.....	6
2.2.2 Gefahr des Überwachungsstaats.....	8
2.2.2 Allgemeine Anmerkungen.....	8
3 Fazit und Zusammenfassung.....	10

# 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

Das Bundeskriminalamt (BKA) soll im Rahmen seiner Aufgabe nach § 5 Absatz 1 Satz 2 BKAG – der Abwehr internationaler terroristischer Gefahren – mit zwei neuen zentralen Befugnissen ausgestattet werden: einem automatisierten biometrischen Abgleich mit öffentlich zugänglichen Internetdaten (§ 39a BKAG-E) sowie einer weitreichenden automatisierten Datenanalyse (§ 39b BKAG-E).

Der Gesetzentwurf begründet diese Erweiterung mit einer „hohen abstrakten Bedrohungslage“ durch internationalen Terrorismus und verweist auf mehrere Gewalttaten durch Einzeltäter im öffentlichen Raum. Unbestritten ist, dass Sicherheitsbehörden zur Terrorismusabwehr auf technische Instrumente angewiesen sind. In einem Rechtsstaat bedarf der Einsatz solcher Mittel jedoch einer strikten Prüfung ihrer Verhältnismäßigkeit.

Der Entwurf verschiebt dieses Gleichgewicht erkennbar: Er transformiert die digitale Öffentlichkeit in einen potenziell permanent auswertbaren Datenraum staatlicher Sicherheitsbehörden. Damit geht eine strukturelle Verschiebung im Verhältnis zwischen Staat und Bürgerinnen und Bürgern einher, also weg vom Grundsatz des Vertrauens, hin zu einem generalisierten Verdacht und einer latenten Beobachtbarkeit.

Die informationelle Selbstbestimmung tritt dabei in den Hintergrund. Die vorgesehenen Befugnisse ermöglichen es, auch unbeteiligte Personen in großem Umfang in Analyse- und Fahndungsprozesse einzubeziehen. Angesichts potenziell niedriger Trefferquoten und systemimmanenter Fehlerrisiken greifen die Maßnahmen tief in die Grundrechte einer Vielzahl von Menschen ein, ohne dass diese selbst Anlass für staatliche Maßnahmen gegeben haben.

Zwar knüpft der Referentenentwurf formal an die Rechtsprechung des Bundesverfassungsgerichts und unionsrechtliche Vorgaben an, die vorgesehenen Instrumente sind jedoch unzureichend durch verfahrensrechtliche Sicherungen sowie Transparenz- und Kontrollmechanismen abgesichert.

Insbesondere die biometrische Internetrecherche, die Einbindung von Drittstaaten, die umfassende verfahrensübergreifende Datenanalyse sowie das Fehlen von Befristungs- und Evaluierungsvorgaben werfen erhebliche rechtsstaatliche und grundrechtliche Bedenken auf.

Der Entwurf verzichtet ausdrücklich auf eine Befristung und Evaluierung der neuen Befugnisse. Angesichts der Dynamik KI-gestützter Analyseverfahren und ihres teils experimentellen Charakters wäre es sachgerecht, diese Instrumente zunächst zeitlich zu begrenzen und an klare Evaluationskriterien zu knüpfen.

Die dauerhafte Etablierung ohne verbindliche Rücknahme- oder Korrekturmechanismen birgt das Risiko einer strukturellen Verfestigung staatlicher Überwachungsbefugnisse – mit entsprechend hohen Hürden für eine spätere Einschränkung. Dies steht im Spannungsverhältnis

zu einer verantwortungsethischen Sicherheitspolitik, die Unsicherheiten und mögliche Fehlentwicklungen systematisch mitdenkt.

## **2.1 Automatisierter biometrischer Internetabgleich (§ 39a BKAG-E)**

Das BKA dürfte über § 39a BKAG-E öffentlich zugängliche personenbezogene Daten mit biometrischen Merkmalen (vor allem Gesichter) aus dem Internet erheben und mit Daten abzugleichen, auf die es zur Erfüllung seiner Aufgaben zugreifen darf, einschließlich weiterer zu diesem Zweck erhobener Internet-Datensätze. Erfasst werden damit also auch Bilder und Videos aus sozialen Netzwerken, Videoplattformen, Nachrichtenportalen oder anderen frei zugänglichen Webseiten, solange sie nicht auf einen eingegrenzten, kontrollierten Personenkreis beschränkt sind.

Obwohl der Normzweck auf die Abwehr von Gefahren des internationalen Terrorismus und die im Zusammenhang damit stehenden Straftaten nach § 5 Absatz 1 Satz 2 BKAG begrenzt ist, werden faktisch die Gesichter einer nicht näher umrissenen Öffentlichkeit zu potenziellem Referenzmaterial polizeilicher biometrischer Suchläufe. Die Betroffenen erfahren von der Erhebung und Verwendung ihrer öffentlich einsehbaren Bilder nichts; sie haben ihre Daten zur privaten oder öffentlichen Kommunikation, nicht aber zur Nutzung in polizeilichen Fahndungsinstrumenten zur Verfügung gestellt.

Die Maßnahme setzt voraus, dass sie zur Identifizierung, Aufenthaltsermittlung, Sachverhaltsaufklärung oder Ermittlung von Zusammenhängen von Straftaten dient und eine im Einzelfall bestehende Gefahr für besonders gewichtige Rechtsgüter (Bestand oder Sicherheit des Bundes oder eines Landes, Leib, Leben, Freiheit, bedeutende Sachwerte) im Zusammenhang mit den in § 5 Absatz 1 Satz 2 genannten Straftaten vorliegt. Zusätzlich ist gefordert, dass die Abwehr der Gefahr auf andere Weise aussichtslos oder wesentlich erschwert wäre; in der präventiven Variante genügt, dass Tatsachen die Annahme rechtfertigen oder das individuelle Verhalten die konkrete Wahrscheinlichkeit begründet, dass innerhalb eines „übersehbaren Zeitraums“ eine entsprechende Straftat begangen wird.

Der Begriff des „übersehbaren Zeitraums“ bleibt unbestimmt und wird auch in den Gesetzesmaterialien nicht genauer definiert. Gleiches gilt für die Formulierung, dass „Tatsachen die Annahme rechtfertigen“ – eine aus der Gefahrenabwehr bekannte relativ niedrige Eingriffsschwelle, die stark von Prognosepraxis und behördlicher Bewertung abhängt. Vor dem Hintergrund des sehr eingriffsintensiven Charakters biometrischer Massenabgleiche erscheint diese Schwellenkonstruktion verfassungsrechtlich anfällig, insbesondere im Lichte der Anforderungen des Bundesverfassungsgerichts an hinreichend konkretisierte Gefahrenlagen bei besonders eingriffsintensiven Überwachungsinstrumenten.

## **2.1.1 Kooperation mit Dritten und Datenübermittlung in Drittstaaten**

§ 39a Absatz 5 BKAG-E erlaubt es dem BKA, den Abgleich durch inländische öffentliche oder nichtöffentliche Stellen oder Stellen anderer EU-Mitgliedstaaten durchführen zu lassen und hierzu die erforderlichen Daten zu übermitteln, wenn der Abgleich intern technisch unmöglich oder nur mit unverhältnismäßig großem Aufwand möglich ist. Absatz 6 geht darüber hinaus und gestattet die Durchführung des Abgleichs durch öffentliche oder nichtöffentliche Stellen in Drittstaaten, wenn dies zum Zweck des Schutzes der nationalen Sicherheit erforderlich ist und bestimmte datenschutzrechtliche Voraussetzungen des BDSG erfüllt sind; gleichzeitig wird eine Abweichung von einzelnen Schutzvorschriften des § 81 BDSG ausdrücklich zugelassen.

Diese Öffnung schafft erhebliche Risiken für die Integrität des europäischen und nationalen Datenschutzniveaus, da biometrische Daten zu Personen in Deutschland in Rechtsräume transferiert werden können, in denen niedrigere materielle und prozedurale Garantien gelten.

Die Norm enthält zwar bestimmte Schutzmechanismen (Verbot des Abgleichs mit Echtzeitdaten, Löschpflicht bei fehlendem Ermittlungsansatz, Protokollierungspflichten, Ausschluss der Nutzung von Daten aus Maßnahmen nach § 12 Absatz 3 BKAG), bleibt aber im Hinblick auf Transparenz und individuellen Rechtsschutz defizitär. Es ist kein grundsätzlicher Richtervorbehalt für den Kern der biometrischen Internetrecherche vorgesehen. Eine richterliche Kontrolle ist ausschließlich für die besonders eingriffsintensive Drittstaatenübermittlung nach Absatz 6 normiert, nicht aber für die Vielzahl der im Inland oder im EU-Ausland durchgeführten Abgleichvorgänge.

Der Entwurf enthält in den neuen Vorschriften keine ausdrückliche Benachrichtigungsregelung für Betroffene. Betroffene haben daher kaum effektive Möglichkeiten, gegen die Nutzung ihrer Daten vorzugehen. Die Annahme des Entwurfs, für Bürgerinnen und Bürger entstehe „kein Erfüllungsaufwand“, verkennt, dass der eigentliche Preis in einer erheblichen Einschränkung der informationellen Selbstbestimmung und faktischen Anonymität im digitalen öffentlichen Raum liegt.

## **2.2 Automatisierte Datenanalyse (§ 39b BKAG-E)**

### **2.2.1 Der Gesetzesentwurf ermöglicht den Aufbau einer dauerhaften Analyseinfrastruktur.**

§ 39b BKAG-E erlaubt dem BKA, Daten, auf die es zur Erfüllung seiner Aufgaben zugreifen darf, mittels einer automatisierten Anwendung zusammenzuführen und zum Zweck der Analyse weiterzuverarbeiten, um Gefahren im Zusammenhang mit Straftaten nach § 5 Absatz 1 Satz 2 BKAG abzuwehren. In der Begründung verweist der Entwurf ausdrücklich auf die Entscheidung des Bundesverfassungsgerichts zur automatisierten Datenanalyse (1 BvR 1547/19, 1 BvR 2634/20) und betont, dass der Einsatz auf hinreichend konkretisierte Gefahren für besonders gewichtige Rechtsgüter beschränkt sei.



Gleichzeitig gestattet Absatz 3, Datensätze aus gezielten, auch automatisierten Abfragen in sonstigen staatlichen Registern sowie im Einzelfall erhobene Datensätze aus Internetquellen in die Weiterverarbeitung einzubeziehen. Damit wird eine technische Infrastruktur etabliert, in der verschiedene Datenquellen zu Analysezielen verbunden und algorithmisch ausgewertet werden können, auch wenn der konkrete Anlassfall jeweils erst durch eine Anordnung nach Absatz 7 freigeschaltet wird. Diese Entkopplung von technischer Vorhaltung und anlassbezogener Analyse verstärkt die Gefahr eines schleichenden Funktionswandels hin zu immer breiterer, weniger strikt anlassbezogener „präventiver Datenfahndung“.

Absatz 4 benennt ausdrücklich, dass im Rahmen der Weiterverarbeitung Beziehungen und Zusammenhänge zwischen Verfahren, Personen, Gruppen, Institutionen, Organisationen, Objekten und Sachen datei- und informationssystemübergreifend identifiziert, klassifiziert, strukturell analysiert und visualisiert werden dürfen; darüber hinaus sind eine Filterung „unbedeutender“ Informationen, die Zuordnung neuer Erkenntnisse zu bekannten Sachverhalten, eine Gewichtung von Suchkriterien sowie statistische Auswertungen vorgesehen. Dies eröffnet der Polizei eine qualitativ neue Form der Wissensproduktion aus vorhandenen Daten, die weit über lineare Recherchen hinausgeht und komplexe Muster-, Netzwerks- und Verhaltensanalysen ermöglicht.

Gerade im Bereich des internationalen Terrorismus, in dem häufig in dezentralen Strukturen und losen Netzwerken agiert wird, kann ein solches Instrument zwar erhebliche Ermittlungsgewinne versprechen, erhöht aber zugleich das Risiko, dass aus der Kombination vieler Teilinformationen sensible Persönlichkeitsprofile und Profile des sozialen Umfelds gebildet werden. Der Entwurf übernimmt hier zwar die vom Bundesverfassungsgericht geforderten materiellen Eingriffsschwellen, übersetzt sie aber nicht in zusätzliche verfahrensrechtliche Sicherungen (z. B. externe Vorabkontrollen, regelmäßige Evaluierung, strikte Nutzungslimits) für diesen besonders eingriffsintensiven Analyseschritt.

§ 39b Absatz 5 verpflichtet das BKA, sicherzustellen, dass diskriminierende Algorithmen weder „hausgebildet noch verwendet werden“, und stellt klar, dass eine ausschließlich auf der Datenanalyse beruhende automatisierte Entscheidungsfindung mit unmittelbaren Rechtsfolgen unzulässig ist. Der Entwurf normiert zwar einzelne Schutzvorgaben, enthält aber keine näheren, eigens ausformulierten Anforderungen an Risikomanagement, Bias-Prüfung, Audits oder Transparenz der eingesetzten Systeme.

Es gibt keine externe richterliche Kontrolle. Die Anordnungscompetenz liegt nach § 39b Absatz 7 BKAG-E intern bei der Präsidentin oder dem Präsidenten des BKA, ihrer oder seiner Vertretung oder Bediensteten mit Befähigung zum Richteramt.

Der Entwurf enthält in den neuen Vorschriften keine ausdrückliche Benachrichtigungsregelung für Betroffene. Der Entwurf enthält in den neuen Vorschriften keine eigens geregelten besonderen Rechtsbehelfe, die auf die Besonderheiten automatisierter Analysen (etwa Black-Box-Charakter, statistische Fehlertoleranzen, indirekte Betroffenheit von



Kontaktpersonen) zugeschnitten wären. In der Praxis ist daher zu erwarten, dass selbst gravierende Fehlzuordnungen oder diskriminierende Effekte nur schwer entdeckt und korrigiert werden können und daraus für Betroffene unangenehme Folgen entstehen können, wenn solche Ergebnisse in weitere polizeiliche Bewertungen und Maßnahmen einfließen.

## 2.2.2 Gefahr des Überwachungsstaats

Der Entwurf ergänzt und verschärft den bereits im Parallelentwurf zur „Stärkung der Ermittlungsbefugnisse in der Polizeiarbeit“ angelegten Trend, die digitale Öffentlichkeit – insbesondere Social-Media-Plattformen – zu einer ständig verfügbaren Ermittlungsressource der Sicherheitsbehörden zu machen. Wer sich im Internet zeigt, muss potenziell damit rechnen, algorithmisch identifiziert, in komplexe Datenanalysen einbezogen und mit weiteren Informationen aus polizeilichen Systemen und Registern verknüpft zu werden, sofern ein entsprechender, auch präventiv begründeter Terrorismusbezug angenommen wird.

Dies verschiebt das Verhältnis zwischen Bürger und Staat in Richtung eines generalisierten Misstrauens und einer ständigen potenziellen Beobachtung, Stichwort Überwachungsstaat.

Automatisierte Datenanalysensysteme und biometrische Abgleiche erzeugen typischerweise große Mengen an „Treffern“, die manuell überprüft und in Ermittlungsstrategien eingeordnet werden müssen. Der Entwurf enthält dazu keine näheren Ausführungen zu den personellen und organisatorischen Ressourcen, die für den Betrieb, die Modellpflege, die Qualitätssicherung und die Auswertung der Ergebnisse erforderlich sind, und behauptet zugleich, dass für Bürgerinnen und Bürger kein Erfüllungsaufwand entstehe.

In der Praxis droht die Gefahr, dass Ermittlungsressourcen in erheblichem Umfang an die Bearbeitung algorithmisch generierter Hinweise gebunden werden, während traditionelle Ermittlungsarbeit (Zeugenbefragungen, operative Maßnahmen, internationale Kooperation auf klassischer Grundlage) unter Zeitdruck leidet. Hinzu kommt eine zunehmende Abhängigkeit von komplexen technischen Systemen, deren Funktionsweise (insbesondere bei proprietären KI-Komponenten) für die meisten Anwenderinnen und Anwender im BKA nur begrenzt nachvollziehbar sein wird.

## 2.2.2 Allgemeine Anmerkungen

Wer als Gesetzgeber solche neuen Instrumente einführen will, muss zumindest

1. die Eingriffsschwellen (insbesondere den Begriff des „übersehbaren Zeitraums“ und die Prognosemaßstäbe) präzisieren und anheben,
2. einen regelmäßigen, externen Richtervorbehalt auch für den Kern der Maßnahmen erwägen,
3. strengere materielle und prozedurale Anforderungen an Auslands- und Drittstaatenkooperationen formulieren,
4. spezifische Transparenz-, Audit- und Diskriminierungsschutzpflichten für eingesetzte Analyse- und Erkennungssysteme normieren,
5. sowie eine verbindliche, unabhängige Evaluierung mit klaren Kriterien und gegebenenfalls Befristung vorsehen.



Ohne solche Nachbesserungen erscheint uns der Entwurf in seiner vorliegenden Form hochproblematisch und ist geeignet das Vertrauen in eine verhältnismäßige und grundrechtsorientierte Terrorismusbekämpfung bei den Bürgerinnen und Bürgern nachhaltig zu beschädigen.

## 3 Fazit und Zusammenfassung

Der Referentenentwurf zur Stärkung digitaler Ermittlungsbefugnisse zur Abwehr von Gefahren des internationalen Terrorismus schafft mit den §§ 39a und 39b BKAG-E zwei Instrumente von erheblicher Eingriffstiefe, die in ihrer Kombination eine qualitativ neue Form staatlicher Wissensproduktion über die Bevölkerung ermöglichen. Die digitale Öffentlichkeit wird damit strukturell zu einem permanenten Auswertungsraum des BKA. Wer sich online zeigt, muss damit rechnen, biometrisch erfasst, algorithmisch analysiert und mit Daten aus polizeilichen Systemen und staatlichen Registern verknüpft zu werden, ohne je Anlass zu einer staatlichen Maßnahme gegeben zu haben und ohne davon zu erfahren.

Dieser Entwurf ist dabei nicht isoliert zu betrachten: Parallel wurde ein Referentenentwurf zur Stärkung digitaler Ermittlungsbefugnisse in der allgemeinen Polizeiarbeit vorgelegt, der dieselben Instrumente des biometrischen Internetabgleichs und der automatisierten Datenanalyse auf BKA und Bundespolizei in einem deutlich breiteren Aufgabenspektrum überträgt; wer nur einen der beiden Entwürfe bewertet, unterschätzt die Gesamtarchitektur der hier angelegten, strukturellen Erweiterung staatlicher Überwachungsbefugnisse erheblich.

Der Entwurf knüpft formal an die Rechtsprechung des Bundesverfassungsgerichts an, übersetzt deren Anforderungen jedoch nicht in hinreichende verfahrensrechtliche Sicherungen. Die Eingriffsschwellen, insbesondere der Begriff des "übersehbaren Zeitraums" und die Prognosemaßstäbe für den präventiven Einsatz, sind normativ zu unscharf, um die vom BVerfG geforderte hinreichende Konkretisierung der Gefahrenlage bei besonders eingriffsintensiven Maßnahmen zu gewährleisten. Wir fordern, dass diese Begriffe durch objektivierbare, normativ klar gefasste Kriterien ersetzt werden.

Für den Kern der biometrischen Internetrecherche nach § 39a BKAG-E ist kein Richtervorbehalt vorgesehen. Ein solcher ist lediglich für die Drittstaatenübermittlung nach Absatz 6 normiert, also für einen Randbereich der Maßnahme. Angesichts der Eingriffsintensität eines biometrischen Massenabgleichs, der unbeteiligte Personen in großem Umfang erfasst, ist die interne Anordnungscompetenz rechtsstaatlich nicht ausreichend. Wir fordern einen obligatorischen Richtervorbehalt für alle Konstellationen des biometrischen Internetabgleichs.

Die Einbindung nichtöffentlicher Stellen und ausländischer Drittstaaten in die Durchführung des Abgleichs nach § 39a Absätze 5 und 6 BKAG-E birgt das Risiko, dass biometrische Daten von in Deutschland lebenden Personen in Rechtsräume mit niedrigeren materiellen und prozeduralen Schutzstandards transferiert werden. Wir fordern strenge, normativ ausformulierte Anforderungen an die Auswahl, Auditierung und datenschutzrechtliche Bindung aller externen Partner sowie eine klare Begrenzung der Drittstaatenkooperation auf nachweislich gleichwertige Schutzstandards.



Für die automatisierte Datenanalyse nach § 39b BKAG-E fehlen eigens ausformulierte Anforderungen an Risikomanagement, Bias-Prüfung und Systemtransparenz. Das pauschale Verbot diskriminierender Algorithmen in Absatz 5 ist ohne konkrete Prüf- und Auditpflichten nicht operationalisierbar. Wir fordern verbindliche, regelmäßige externe Audits der eingesetzten Analyse- und Erkennungssysteme sowie eine gesetzlich verankerte Pflicht zur Offenlegung der wesentlichen Funktionsparameter gegenüber den Datenschutzbehörden.

Schließlich verzichtet der Entwurf vollständig auf eine Befristung und unabhängige Evaluierung der neuen Befugnisse. Angesichts des experimentellen Charakters KI-gestützter Analyseverfahren und ihrer systemimmanenten Fehlerrisiken ist die dauerhafte Etablierung ohne normierte Rücknahme- oder Korrekturmechanismen verantwortungsethisch nicht vertretbar. Wir fordern eine verpflichtende, befristete Erprobungsphase mit klar definierten Evaluationskriterien und der ausdrücklichen gesetzlichen Option zur Rücknahme, bevor diese Befugnisse dauerhaft in Kraft treten.

In seiner vorliegenden Form ist der Entwurf geeignet, das Vertrauen der Bevölkerung in eine verhältnismäßige und grundrechtsorientierte Sicherheitspolitik nachhaltig zu beschädigen. Ohne die genannten Nachbesserungen lehnen wir ihn ab.