

## Gesetzentwurf der Bundesregierung

### Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse zur Abwehr von Gefahren des internationalen Terrorismus

#### A. Problem und Ziel

Polizei- und Strafverfolgungsbehörden müssen zum Schutz der Inneren Sicherheit stetig auf neue Herausforderungen reagieren. Die Bundesrepublik Deutschland sowie ihre Interessen und Einrichtungen weltweit stehen unverändert im Zielspektrum unterschiedlicher terroristischer Organisationen, allen voran des sogenannten „Islamischen Staats“ mit seinen Regionalorganisationen. Die nationale Sicherheitslage wird dabei mitunter durch internationale Konflikte, wie beispielsweise im Nahen und Mittleren Osten, verschärft. In den vergangenen Jahren kam es im öffentlichen Raum vermehrt zu schweren Gewalttaten durch Einzeltäter mit verschiedenen Motivationslagen. Es besteht eine hohe abstrakte Bedrohungslage für die Sicherheit in Deutschland – insbesondere durch den internationalen Terrorismus.

Die Bedrohung durch terroristische und kriminelle Strukturen erfordert den Einsatz technologischer Instrumente – auch Künstlicher Intelligenz – sowie die Verfügbarkeit notwendiger Daten. Ziel des Gesetzentwurfs ist es, dem Bundeskriminalamt die rechtlichen Befugnisse zur Verfügung zu stellen, um den Herausforderungen sachgerecht begegnen zu können.

#### B. Lösung

Der Gesetzentwurf enthält Befugnisse für das Bundeskriminalamt. Der Gesetzentwurf bildet ein Paket mit dem Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit.

Die automatisierte Datenanalyse ist ein zentraler Baustein, um die stetig wachsenden Datenmengen in polizeilichen Ermittlungsverfahren verarbeiten zu können. Mittels der Analyse bereits rechtmäßig erhobener polizeilicher Daten ist es möglich, Verbindungen zwischen Taten, Personen, Orten sowie an deren Anknüpfungspunkten zu finden. Insbesondere für komplexe Ermittlungen in der Terrorismusabwehr, ist die automatisierte Datenanalyse als Ermittlungsinstrument notwendig. Überdies ermöglicht sie es, in konkreten Anschlagssituationen schnellstmöglich Daten auszuwerten und somit weitere Maßnahmen zur Gefahrenabwehr zu ergreifen.

Der biometrische Abgleich mit öffentlich zugänglichen Daten aus dem Internet ist erforderlich, um Personen insbesondere zu identifizieren, lokalisieren sowie Tat-Täter-Zusammenhänge zu erschließen. Die Befugnis erlaubt es, biometrische Daten – zum Beispiel das Lichtbild einer gesuchten Person – mit öffentlich zugänglichen Daten aus dem Internet abzugleichen. Im Rahmen der Ausübung der Befugnis ist die Zusammenarbeit mit Dritten, auch außerhalb der Europäischen Union, erlaubt.

Zudem enthält der Gesetzentwurf das Instrument der Sicherungsanordnung für das Bundeskriminalamt. Damit kann es die Sicherung von Verkehrsdaten veranlassen, sofern und solange die rechtlichen oder tatsächlichen Voraussetzungen einer Datenerhebung noch nicht vorliegen. Das Bundeskriminalamt erhält die Befugnis für die Wahrnehmung der Aufgabe als Zentralstelle sowie zur Abwehr von Gefahren des internationalen Terrorismus.

Die Befugnisse sind technik- und produktneutral ausgestaltet.

### **C. Alternativen**

Keine.

### **D. Haushaltsausgaben ohne Erfüllungsaufwand**

Die notwendigen Haushaltsausgaben für die Umsetzung der Befugnisse des Bundeskriminalamts zum biometrischen Internetabgleich sowie zur automatisierten Datenanalyse sind vollumfänglich vom Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit umfasst. Für die Befugnisse zur Sicherungsanordnung lässt sich der Mehrbedarf derzeit nicht beziffern.

Sofern hier weiterer Mehrbedarf an Sach- und Personalmitteln sowie an Planstellen und Stellen für das Bundeskriminalamt entsteht und haushaltswirksam wird, ist dieser Gegenstand künftiger Haushaltsaufstellungsverfahren.

### **E. Erfüllungsaufwand**

#### **E.1 Erfüllungsaufwand für Bürgerinnen und Bürger**

Für Bürgerinnen und Bürger entsteht kein Erfüllungsaufwand.

#### **E.2 Erfüllungsaufwand für die Wirtschaft**

Für die Wirtschaft entsteht kein Erfüllungsaufwand.

#### **Davon Bürokratiekosten aus Informationspflichten**

Keine.

#### **E.3 Erfüllungsaufwand der Verwaltung**

Für die Verwaltung entsteht kein Erfüllungsaufwand.

**F. Weitere Kosten**

Keine.

*Vorabfassung – wird durch die lektorierte Fassung ersetzt.*

**BUNDESREPUBLIK DEUTSCHLAND  
DER BUNDESKANZLER**

Berlin, 26. Mai 2026

An die  
Präsidentin des  
Deutschen Bundestages  
Frau Julia Klöckner  
Platz der Republik 1  
11011 Berlin

Sehr geehrte Frau Bundestagspräsidentin,

hiermit übersende ich den von der Bundesregierung beschlossenen

Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse zur  
Abwehr von Gefahren des internationalen Terrorismus

mit Begründung und Vorblatt (Anlage 1).

Ich bitte, die Beschlussfassung des Deutschen Bundestages herbeizuführen.

Federführend ist das Bundesministerium des Innern.

Die Stellungnahme des Nationalen Normenkontrollrates gemäß § 6 Absatz 1 NKRG  
ist als Anlage 2 beigefügt.

Die Stellungnahme der Bundesregierung zur Stellungnahme des Nationalen  
Normenkontrollrates ist als Anlage 3 beigefügt.

Der Gesetzentwurf ist dem Bundesrat am 1. Mai 2026 als besonders eilbedürftig  
zugeleitet worden.

Die Stellungnahme des Bundesrates zu dem Gesetzentwurf sowie die Auffassung der  
Bundesregierung zu der Stellungnahme des Bundesrates werden unverzüglich  
nachgereicht.

Mit freundlichen Grüßen  
Friedrich Merz

*Vorabfassung – wird durch die lektorierte Fassung ersetzt.*

## Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse zur Abwehr von Gefahren des internationalen Terrorismus

Vom ...

Der Bundestag hat mit Zustimmung des Bundesrates das folgende Gesetz beschlossen:

### Artikel 1

#### Änderung des Bundeskriminalamtgesetzes

Das Bundeskriminalamtgesetz vom 1. Juni 2017 (BGBl. I S. 1354; 2019 I S. 400), das zuletzt durch ... geändert worden ist, wird wie folgt geändert:

1. Die Inhaltsübersicht wird wie folgt geändert:
  - a) Nach der Angabe zu § 10a wird die folgende Angabe eingefügt:  
„§ 10b Sicherung von Verkehrsdaten“.
  - b) Nach der Angabe zu § 39 werden die folgenden Angaben eingefügt:  
„§ 39a Automatisierter biometrischer Abgleich mit öffentlich zugänglichen Daten aus dem Internet  
§ 39b Automatisierte Datenanalyse“.
  - c) Nach der Angabe zu § 87 wird die folgende Angabe eingefügt:  
„§ 87a Bußgeldvorschriften“.
2. Nach § 10a wird der folgende § 10b eingefügt:

#### „§ 10b

#### Sicherung von Verkehrsdaten

(1) Das Bundeskriminalamt kann zur Erfüllung der Aufgabe als Zentralstelle zum Zweck einer etwaigen Erhebung gegenüber demjenigen, der öffentlich zugängliche Telekommunikationsdienste anbietet oder daran mitwirkt, anordnen, Verkehrsdaten nach § 3 Nummer 70 des Telekommunikationsgesetzes von betroffenen Personen unverzüglich zu sichern, wenn

1. die zuständige Strafverfolgungsbehörde oder die zuständige Polizeibehörde noch nicht erkennbar ist und
  - a) zureichende tatsächliche Anhaltspunkte dafür vorliegen, dass eine Straftat begangen worden ist, die eine Erhebung der Verkehrsdaten nach § 100g Absatz 1 bis 4 der Strafprozessordnung rechtfertigen würde,
  - b) tatsächliche Anhaltspunkte dafür vorliegen, dass eine Person innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Absatz 2 der Strafprozessordnung bezeichnete Straftat, begehen wird und
    - aa) nach Feststellung der Zuständigkeit einer Landespolizeibehörde eine Erhebung durch diese nach den für sie geltenden Vorschriften ermöglicht werden kann oder

- bb) nach Feststellung der Zuständigkeit des Bundeskriminalamtes gemäß § 5 Absatz 1 eine Erhebung nach § 52 Absatz 1 ermöglicht werden kann, oder
- c) tatsächliche Anhaltspunkte dafür vorliegen, dass eine Person mit einer Person nach Nummer 1 Buchstabe b in nicht nur flüchtigem oder in zufälligem Kontakt und in einer Weise in Verbindung steht, die die Annahme rechtfertigt, dass nach Gewinnung weiterer Erkenntnisse
  - aa) nach Feststellung der Zuständigkeit einer Landespolizeibehörde eine Erhebung durch diese nach den für sie geltenden Vorschriften ermöglicht werden kann oder
  - bb) nach Feststellung der Zuständigkeit des Bundeskriminalamtes gemäß § 5 Absatz 1 eine Erhebung nach § 52 Absatz 1 ermöglicht werden kann, und
- 2. die betroffene Person in den Fällen der Nummer 1 Buchstabe a und b in einem persönlichen oder räumlichen Bezug zu der Straftat steht und
- 3. die Daten für die jeweiligen Zwecke der Erhebung von Bedeutung sein können.

(2) Die Maßnahme darf nur durch die zuständige Abteilungsleitung des Bundeskriminalamtes oder deren Vertretung angeordnet werden. Die zuständige Abteilungsleitung kann die Anordnungsbefugnis auf Bedienstete des Bundeskriminalamtes mit Befähigung zum Richteramt übertragen.

(3) Die Anordnung ergeht schriftlich. In ihr sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich mit Namen und Anschrift,
2. die Rufnummer oder eine andere Kennung des betroffenen Anschlusses oder Endgerätes, sofern sich nicht aus bestimmten Tatsachen ergibt, dass diese zugleich einem anderen Endgerät zugeordnet ist,
3. Art, Umfang und Dauer der Maßnahme unter Benennung des Endzeitpunktes,
4. Art der durch die Maßnahme zu erhebenden Daten und ihre voraussichtliche Bedeutung für den Zweck der Erhebung sowie
5. die wesentlichen Gründe für die Anordnung der Maßnahme.

Abweichend von Satz 2 Nummer 2 genügt bei der Sicherung von Daten einer Funkzelle eine räumlich und zeitlich hinreichende Bezeichnung der Telekommunikation, sofern anderenfalls die Erreichung des Zwecks der Maßnahme aussichtslos oder wesentlich erschwert wäre.

(4) Die Anordnung ist auf höchstens drei Monate zu befristen. Das Bundeskriminalamt informiert nach Feststellung der Zuständigkeit eines Landes die zuständige Landespolizeibehörde über die Anordnung.

(5) Der auf Grund einer Sicherungsanordnung nach Absatz 1 Verpflichtete hat die von der Anordnung erfassten Daten unverzüglich und vollständig zu sichern. Ob und in welchem Umfang für die unverzügliche Sicherung nach Absatz 1 Vorkehrungen zu treffen sind, bestimmt sich nach dem Telekommunikationsgesetz und der Telekommunikations-Überwachungsverordnung. Der Umfang der Entschädigung bemisst sich nach § 23 und Anlage 3 des Justizvergütungs- und -entschädigungsgesetzes.“

3. Nach § 39 werden die folgenden §§ 39a, 39b eingefügt:

„§ 39a

Automatisierter biometrischer Abgleich mit öffentlich verfügbaren Daten aus dem Internet

(1) Das Bundeskriminalamt kann öffentlich zugängliche personenbezogene Daten, die biometrische Merkmale enthalten, aus dem Internet erheben und mit Daten, auf die es zur Erfüllung seiner Aufgaben zugreifen darf, mittels einer automatisierten Anwendung zur Datenverarbeitung biometrisch abgleichen, sofern

1. dies zum Zweck der Identifizierung, Aufenthaltsermittlung, Erforschung des Sachverhalts oder Ermittlung von Zusammenhängen von Straftaten oder Gefahren erforderlich ist und

- a) eine im Einzelfall bestehenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, im Zusammenhang mit Straftaten nach § 5 Absatz 1 Satz 2 besteht,
  - b) Tatsachen die Annahme rechtfertigen, dass eine Person innerhalb eines übersichtbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Straftat nach § 5 Absatz 1 Satz 2 begehen wird, oder
  - c) das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersichtbaren Zeitraums eine Straftat nach § 5 Absatz 1 Satz 2 begehen wird, und
2. die Abwehr der Gefahr oder die Verhütung der Straftat auf andere Weise aussichtslos ist oder wesentlich erschwert wäre.

Ein Abgleich mit öffentlich zugänglichen Echtzeitdaten ist unzulässig.

(2) Die Maßnahme nach Absatz 1 Satz 1 darf durchgeführt werden gegen

1. die entsprechend § 18 oder § 19 des Bundespolizeigesetzes Verantwortlichen oder Personen im Sinne von Absatz 1 Satz 1 Nummer 1 Buchstabe b oder c und
2. Personen entsprechend § 21 des Bundespolizeigesetzes, sofern überwiegende schutzwürdige Interessen dieser Personen nicht entgegenstehen.

(3) Für die nach Absatz 1 Satz 1 abzugleichenden Daten ist § 12 Absatz 2 anzuwenden. Der Abgleich mit Daten, die die aus in § 12 Absatz 3 genannten Maßnahmen erlangt wurden, ist ausgeschlossen.

(4) Die im Rahmen des biometrischen Abgleichs nach Absatz 1 Satz 1 erhobenen und verarbeiteten Daten sind nach dessen Durchführung unverzüglich zu löschen, sofern sie keinen konkreten Ermittlungsansatz für den Ausgangssachverhalt oder ein anderes Verfahren aufweisen. Durch organisatorische und technische Maßnahmen hat das Bundeskriminalamt zu gewährleisten, dass die Daten gegen unbefugte Kenntnisnahme geschützt sind. Für die Protokollierung der Verarbeitungsschritte gilt § 82 Absatz 1. Zudem ist die Zielperson zu protokollieren.

(5) Das Bundeskriminalamt kann den Abgleich durch eine inländische öffentliche oder nichtöffentliche Stelle oder eine öffentliche oder nichtöffentliche Stelle eines Mitgliedsstaats der Europäischen Union durchführen lassen, hierzu an diese Stelle erforderliche Daten übermitteln und, sofern erforderlich, von § 25 Absatz 6, auch in Verbindung mit § 26, abweichen, wenn

1. die Voraussetzungen des Absatzes 1 Satz 1 erfüllt sind und
2. der Abgleich durch das Bundeskriminalamt selbst technisch unmöglich oder nur mit unverhältnismäßig großem Aufwand möglich ist.

(6) Das Bundeskriminalamt kann den Abgleich durch eine öffentliche oder nichtöffentliche Stelle in einem Drittstaat durchführen lassen und hierzu an diese Stelle erforderliche Daten übermitteln, wenn

1. dies zum Zweck des Schutzes der nationalen Sicherheit erforderlich ist,
2. die Voraussetzungen des Absatzes 1 Satz 1 sowie vorbehaltlich des Satzes 2 die Voraussetzungen des § 27 Absatz 8 und des § 81 des Bundesdatenschutzgesetzes erfüllt sind und
3. der Abgleich durch das Bundeskriminalamt selbst oder eine inländische öffentliche oder nichtöffentliche Stelle oder eine öffentliche oder nichtöffentliche Stelle eines Mitgliedsstaats der Europäischen Union technisch unmöglich oder nur mit unverhältnismäßig großem Aufwand möglich ist.

Sofern dies erforderlich ist, darf das Bundeskriminalamt von § 81 Absatz 1 Nummer 3 und Absatz 4 des Bundesdatenschutzgesetzes abweichen.

(7) Die §§ 25 bis 28 bleiben im Übrigen unberührt.

(8) Die Maßnahme nach Absatz 6 darf nur auf Antrag der Präsidentin oder des Präsidenten des Bundeskriminalamtes oder ihrer oder seiner Vertretung durch das Gericht angeordnet werden. Bei Gefahr im

Verzug kann die Anordnung durch die Präsidentin oder den Präsidenten des Bundeskriminalamtes oder ihre oder seine Vertretung getroffen werden. In diesem Fall ist die gerichtliche Entscheidung unverzüglich nachzuholen. Soweit die Anordnung nicht binnen drei Tagen durch das Gericht bestätigt wird, tritt sie außer Kraft. Die Präsidentin oder der Präsident des Bundeskriminalamtes kann die Antragsbefugnis nach Satz 1 sowie die Anordnungsbefugnis nach Satz 2 auf Bedienstete des Bundeskriminalamtes mit Befähigung zum Richteramt übertragen.

### § 39b

#### Automatisierte Datenanalyse

(1) Das Bundeskriminalamt kann Daten, auf die es zur Erfüllung seiner Aufgaben zugreifen darf, nach Maßgabe von § 12 mittels einer automatisierten Anwendung zur Datenverarbeitung zusammenführen und darüber hinaus zum Zwecke der Analyse weiterverarbeiten, sofern dies zur Abwehr einer im Einzelfall bestehenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, im Zusammenhang mit Straftaten nach § 5 Absatz 1 Satz 2 erforderlich ist. Eine Maßnahme nach Satz 1 ist auch zulässig, sofern

1. Tatsachen die Annahme rechtfertigen, dass eine Person innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Straftat nach § 5 Absatz 1 Satz 2 begehen wird oder
2. das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums eine Straftat nach § 5 Absatz 1 Satz 2 begehen wird

und dies zur Verhütung dieser Straftat erforderlich ist. Die nach Satz 1 mittels einer automatisierten Anwendung zur Datenverarbeitung zusammengeführten Daten dürfen ferner für Zwecke der Strafverfolgung gemäß § 4 nach Maßgabe von § 98e der Strafprozessordnung weiterverarbeitet werden.

(2) Der Abgleich nach Absatz 1 darf durchgeführt werden gegen

1. die entsprechend § 18 oder § 19 des Bundespolizeigesetzes Verantwortlichen oder Personen im Sinne von Absatz 1 Satz 2 Nummer 1 oder 2 und
2. Personen entsprechend § 21 des Bundespolizeigesetzes, sofern überwiegende schutzwürdige Interessen dieser Personen nicht entgegenstehen.

(3) Eine direkte Anbindung der Anwendung zur automatisierten Datenanalyse an Register, die nicht in den Anwendungsbereich der Richtlinie (EU) 2016/680 fallen, und an Internetdienste ist unzulässig. Datensätze aus gezielten, auch automatisierten Abfragen in sonstigen staatlichen Registern und im Einzelfall erhobene Datensätze aus Internetquellen können in die Weiterverarbeitung einbezogen werden.

(4) Im Rahmen der Weiterverarbeitung nach Absatz 1 können insbesondere

1. datei- und informationssystemübergreifend Beziehungen oder Zusammenhänge zwischen Verfahren, Vorgängen, Personen, Personengruppierungen, Institutionen, Organisationen, Orten, Objekten und Sachen identifiziert und hergestellt, sowohl qualitativ als auch quantitativ klassifiziert, strukturell analysiert und visualisiert werden,
2. für die Erreichung des Zwecks der Weiterverarbeitung nach Absatz 1 unbedeutende Informationen und Erkenntnisse ausgeschlossen werden,
3. die eingehenden Erkenntnisse zu bekannten Sachverhalten zugeordnet werden,
4. Suchkriterien, insbesondere nach Sachnähe, Aktualität und Erheblichkeit der Verknüpfung mit anderen Informationen bezogen auf den Zweck der Weiterverarbeitung nach Absatz 1, gewichtet werden sowie
5. gespeicherte Daten statistisch ausgewertet werden.

(5) Das Bundeskriminalamt hat bei der Weiterverarbeitung nach Absatz 1 sicherzustellen, dass diskriminierende Algorithmen weder herausgebildet noch verwendet werden. § 12 und § 22 Absatz 2 sowie Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung bleiben unberührt. 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.

(6) Das Bundeskriminalamt gewährleistet im Rahmen der Regelung der Zugriffsberechtigungen nach § 15, dass das für die Durchführung der Maßnahme nach Absatz 1 eingesetzte Personal besonders geschult wird. Durch organisatorische und technische Maßnahmen hat das Bundeskriminalamt zu gewährleisten, dass die Daten gegen unbefugte Kenntnisnahme geschützt sind. Für die Protokollierung der Zugriffe und Verarbeitungsschritte gilt § 82 Absatz 1. Zudem ist die Zielperson zu protokollieren. Die Übermittlung von personenbezogenen Daten an andere Stellen zur Durchführung der automatisierten Datenanalyse nach Absatz 1 ist ausgeschlossen.

(7) Die Maßnahme nach Absatz 1 ist durch die Präsidentin oder den Präsidenten des Bundeskriminalamtes oder ihrer oder seiner Vertretung oder durch eine Bedienstete oder einen Bediensteten des Bundeskriminalamtes mit Befähigung zum Richteramt anzuordnen.“

4. § 52 wird wie folgt geändert:

a) Absatz 1 wird durch den folgenden Absatz 1 ersetzt:

„(1) Wenn die Abwehr der Gefahr oder Verhütung der Straftaten auf andere Weise aussichtslos oder wesentlich erschwert wäre, kann das Bundeskriminalamt ohne Wissen der betroffenen Person bei demjenigen, der öffentlich zugängliche Telekommunikationsdienste anbietet oder daran mitwirkt, zu folgenden Personen Verkehrsdaten nach § 3 Nummer 70 des Telekommunikationsgesetzes erheben:

1. den entsprechend § 18 oder § 19 des Bundespolizeigesetzes Verantwortlichen zur Abwehr einer dringenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist,
2. Personen, bei denen bestimmte Tatsachen die Annahme rechtfertigen, dass sie innerhalb eines übersichtbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Straftat nach § 5 Absatz 1 Satz 2 begehen werden,
3. Personen, deren individuelles Verhalten die konkrete Wahrscheinlichkeit begründen, dass sie innerhalb eines übersichtbaren Zeitraums eine Straftat nach § 5 Absatz 1 Satz 2 begehen werden,
4. Personen, bei denen bestimmte Tatsachen die Annahme rechtfertigen, dass sie für eine Person nach Nummer 1 bestimmte oder von dieser herrührende Mitteilungen entgegennehmen oder weitergeben, oder
5. Personen, bei der bestimmte Tatsachen die Annahme rechtfertigen, dass eine Person nach Nummer 1 deren Telekommunikationsanschluss oder Endgerät benutzen werden.“

b) Nach Absatz 2 wird der folgende Absatz 3 eingefügt:

„(3) Zum Zwecke einer etwaigen Erhebung nach Absatz 1 darf das Bundeskriminalamt anordnen, dass Verpflichtete nach Absatz 1 Verkehrsdaten von betroffenen Personen unverzüglich zu sichern haben, wenn die betroffene Person in einem persönlichen oder räumlichen Bezug zu der Gefahr oder zu verhütenden Straftat nach Absatz 1 Satz 1 steht und

1. tatsächliche Anhaltspunkte dafür vorliegen, dass es sich um eine Person im Sinne des Absatzes 1 handelt und eine Erhebung nach Absatz 1 gerechtfertigt sein könnte, oder
2. tatsächliche Anhaltspunkte dafür vorliegen, dass es sich um eine Person handelt, die mit einer Person nach Absatz 1 Nummer 2 oder 3 in nicht nur flüchtigem oder in zufälligem Kontakt und in einer Weise in Verbindung steht, welche die Annahme rechtfertigt, dass nach Gewinnung weiterer Erkenntnisse eine Erhebung nach Absatz 1 gerechtfertigt sein könnte.

Die Daten müssen für die in Absatz 1 jeweils genannten Zwecke von Bedeutung sein können.“

- c) Der bisherige Absatz 3 wird zu Absatz 4 und in Satz 1 wird die Angabe „§ 51 Absatz 3 bis 6 gilt“ durch die Angabe „Für Maßnahmen nach den Absätzen 1 und 2 gilt § 51 Absatz 3 bis 6“ ersetzt.
- d) Nach Absatz 4 werden die folgenden Absätze 5 bis 8 eingefügt:

„(5) Die Maßnahme nach Absatz 3 darf nur durch die zuständige Abteilungsleitung des Bundeskriminalamtes oder deren Vertretung angeordnet werden. Die zuständige Abteilungsleitung kann die Anordnungsbefugnis auf Bedienstete des Bundeskriminalamtes mit Befähigung zum Richteramt übertragen.

(6) Die Anordnung nach Absatz 3 ergeht schriftlich. In ihr sind anzugeben:

1. die Person, gegen die sich die Maßnahme richtet, soweit möglich mit Namen und Anschrift,
2. die Rufnummer oder eine andere Kennung des betroffenen Anschlusses oder Endgerätes, sofern sich nicht aus bestimmten Tatsachen ergibt, dass diese zugleich einem anderen Endgerät zugeordnet ist,
3. Art, Umfang und Dauer der Maßnahme unter Benennung des Endzeitpunktes,
4. Art der durch die Maßnahme zu erhebenden Daten und ihre voraussichtliche Bedeutung für den Zweck der Erhebung sowie
5. die wesentlichen Gründe für die Anordnung der Maßnahme.

Abweichend von Satz 2 Nummer 2 genügt bei der Sicherung von Daten einer Funkzelle eine räumlich und zeitlich hinreichende Bezeichnung der Telekommunikation, sofern anderenfalls die Erreichung des Zwecks der Maßnahme aussichtslos oder wesentlich erschwert wäre.

(7) Die Anordnung nach Absatz 5 ist auf höchstens drei Monate zu befristen und darf nur auf Antrag der zuständigen Abteilungsleitung des Bundeskriminalamtes oder deren Vertretung durch das Gericht um höchstens drei Monate verlängert werden.

(8) Der auf Grund einer Anordnung nach Absatz 3 Verpflichtete hat die von der Anordnung erfassten Daten unverzüglich und vollständig zu sichern. Ob und in welchem Umfang für die Maßnahme nach Absatz 3 Vorkehrungen zu treffen sind, bestimmt sich nach dem Telekommunikationsgesetz und der Telekommunikations-Überwachungsverordnung. Der Umfang der Entschädigung bemisst sich nach § 23 und Anlage 3 des Justizvergütungs- und -entschädigungsgesetzes.“

5. Nach § 87 wird der folgende § 87a eingefügt:

„§ 87a

#### Bußgeldvorschriften

- (1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig entgegen § 10b Absatz 5 Satz 1 oder § 52 Absatz 8 Satz 1 die dort genannte Daten nicht, nicht vollständig oder nicht rechtzeitig sichert.
- (2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfhunderttausend Euro geahndet werden.
- (3) Verwaltungsbehörde im Sinne des § 36 Absatz 1 Nummer 1 des Gesetzes über Ordnungswidrigkeiten ist das Bundeskriminalamt.“

## Artikel 2

### Inkrafttreten

Dieses Gesetz tritt am Tag nach der Verkündung in Kraft.

## Begründung

### A. Allgemeiner Teil

#### I. Zielsetzung und Notwendigkeit der Regelungen

Polizei- und Strafverfolgungsbehörden müssen zum Schutz der inneren Sicherheit stetig auf neue Herausforderungen reagieren. Die Bundesrepublik Deutschland sowie ihre Interessen und Einrichtungen weltweit stehen unverändert im Zielspektrum unterschiedlicher terroristischer Organisationen, allen voran des sogenannten „Islamischen Staats“ mit seinen Regionalorganisationen. Die nationale Sicherheitslage wird dabei mitunter durch internationale Konflikte, wie beispielsweise im Nahen und Mittleren Osten, verschärft. In den vergangenen Jahren kam es im öffentlichen Raum vermehrt zu schweren Gewalttaten durch Einzeltäter mit verschiedenen Motivationslagen. Es besteht eine hohe abstrakte Bedrohungslage für die Sicherheit in Deutschland – insbesondere durch den internationalen Terrorismus.

Die Bedrohung durch terroristische und kriminelle Strukturen erfordert den Einsatz technologischer Instrumente – auch Künstlicher Intelligenz – sowie die Verfügbarkeit notwendiger Daten. Ziel des Gesetzentwurfs ist es, dem Bundeskriminalamt die rechtlichen Befugnisse zur Verfügung zu stellen, um den Herausforderungen sachgerecht begegnen zu können.

#### II. Wesentlicher Inhalt des Entwurfs

Der Gesetzentwurf enthält Befugnisse für das Bundeskriminalamt. Der Gesetzentwurf bildet ein Paket mit dem Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit.

Die automatisierte Datenanalyse ist ein zentraler Baustein, um die stetig wachsenden Datenmengen in polizeilichen Ermittlungsverfahren verarbeiten zu können. Mittels der Analyse bereits rechtmäßig erhobener polizeilicher Daten ist es möglich, Verbindungen zwischen Taten, Personen, Orten sowie an deren Anknüpfungspunkten zu finden. Insbesondere für komplexe Ermittlungen in der Terrorismusabwehr, ist die automatisierte Datenanalyse als Ermittlungsinstrument notwendig. Überdies ermöglicht sie es, in konkreten Anschlagssituationen schnellstmöglich Daten auszuwerten und somit weitere Maßnahmen zur Gefahrenabwehr zu ergreifen.

Der biometrische Abgleich mit öffentlich zugänglichen Daten aus dem Internet ist erforderlich, um Personen insbesondere zu identifizieren, lokalisieren sowie Tat-Täter-Zusammenhänge zu erschließen. Die Befugnis erlaubt es, biometrische Daten – zum Beispiel das Lichtbild einer gesuchten Person – mit öffentlich zugänglichen Daten aus dem Internet abzugleichen. Im Rahmen der Ausübung der Befugnis ist die Zusammenarbeit mit Dritten, auch außerhalb der Europäischen Union, erlaubt.

Zudem enthält der Gesetzentwurf das Instrument der Sicherungsanordnung für das Bundeskriminalamt. Damit kann es die Sicherung von Verkehrsdaten veranlassen, sofern und solange die rechtlichen oder tatsächlichen Voraussetzungen einer Datenerhebung noch nicht vorliegen. Das Bundeskriminalamt erhält die Befugnis für die Wahrnehmung der Aufgabe als Zentralstelle sowie zur Abwehr von Gefahren des internationalen Terrorismus.

Die Befugnisse sind technik- und produktneutral ausgestaltet.

#### III. Exekutiver Fußabdruck

Interessenvertreterinnen und Interessenvertreter Dritter oder sonstige Personen außerhalb der Bundesverwaltung sind nicht an der Erstellung des Entwurfs beteiligt worden.

#### IV. Alternativen

Keine.

#### V. Gesetzgebungskompetenz

Die Gesetzgebungskompetenz des Bundes folgt für die Änderung des Bundeskriminalamtgesetzes (BKAG) bezüglich der Abwehr von Gefahren des internationalen Terrorismus aus Artikel 73 Absatz 1 Nummer 9a und bezüglich der Zentralstellenfunktion aus Artikel 73 Absatz 1 Nummer 10 Buchstabe a des Grundgesetzes.

#### VI. Vereinbarkeit mit dem Recht der Europäischen Union und völkerrechtlichen Verträgen

Der Gesetzentwurf ist mit dem Recht der Europäischen Union und völkerrechtlichen Verträgen, die die Bundesrepublik Deutschland geschlossen hat, vereinbar.

#### VII. Gesetzesfolgen

##### 1. Rechts- und Verwaltungsvereinfachung

Der Gesetzentwurf dient dem Schutz der öffentlichen Sicherheit in Deutschland und der Stärkung der Ermittlungsbefugnisse im Rahmen von Gefahrenabwehr.

##### 2. Nachhaltigkeitsaspekte

Der Gesetzentwurf steht im Einklang mit den Leitgedanken der Bundesregierung zur nachhaltigen Entwicklung im Sinne der Deutschen Nachhaltigkeitsstrategie, die der Umsetzung der Agenda 2030 für nachhaltige Entwicklung der Vereinten Nationen dient. Der Entwurf dient entsprechend der Zielvorgabe 16.1 der Erhöhung der persönlichen Sicherheit und dem Schutz vor Kriminalität.

##### 3. Haushaltsausgaben ohne Erfüllungsaufwand

Die notwendigen Haushaltsausgaben für die Umsetzung der Befugnisse des Bundeskriminalamts zum biometrischen Internetabgleich sowie zur automatisierten Datenanalyse sind vollumfänglich vom Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit umfasst. Für die Befugnisse zur Sicherungsanordnung lässt sich der Mehrbedarf derzeit nicht beziffern.

Sofern hier weiterer Mehrbedarf an Sach- und Personalmitteln sowie an Planstellen und Stellen für das Bundeskriminalamt entsteht und haushaltswirksam wird, ist dieser Gegenstand künftiger Haushaltsaufstellungsverfahren.

##### 4. Erfüllungsaufwand

###### a) Erfüllungsaufwand für Bürgerinnen und Bürger

Für Bürgerinnen und Bürger entsteht kein Erfüllungsaufwand.

###### b) Erfüllungsaufwand für die Wirtschaft

Für die Wirtschaft entsteht kein Erfüllungsaufwand.

###### c) Erfüllungsaufwand der Verwaltung

##### 5. Weitere Kosten

Weitere Kosten sind nicht zu erwarten.

## 6. Weitere Gesetzesfolgen

Auswirkungen auf demografierelevante Belange sind nicht zu erwarten.

## VIII. Befristung; Evaluierung

Eine Befristung ist nicht vorgesehen.

Eine Evaluierung der Regelungen dieses Gesetzes ist ebenfalls nicht vorgesehen. Die neuen Regelungen knüpfen an den bestehenden gesetzlichen Aufgaben der Behörden an. Die Anwendung der Befugnisse sowie deren Auswirkung unterliegt einer kontinuierlichen Kontrolle, insbesondere durch die parlamentarische Kontrolle, die Fach- und Rechtsaufsicht sowie die bestehenden Berichtspflichten und gerichtliche Rechtsschutzmöglichkeiten.

### B. Besonderer Teil

#### Zu Artikel 1 (Änderung des Bundeskriminalamtgesetzes)

##### Zu Nummer 1 (Inhaltsübersicht)

##### Zu Buchstabe a

Es handelt sich um redaktionelle Folgeänderung zur Einführung von § 10b.

##### Zu Buchstabe b

Es handelt sich um eine redaktionelle Folgeänderung zur Einführung von §§ 39a, 39b.

##### Zu Buchstabe c

##### Zu Nummer 2 (§ 10b)

Das Bundeskriminalamt hat nach § 2 Absatz 1 die Aufgabe, als Zentralstelle für die Kriminalpolizei die Polizeien des Bundes und der Länder bei der Verhütung, Aufklärung und Verfolgung von Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung zu unterstützen. Aufgrund der Bedeutung von Verkehrsdaten für die Gefahrenabwehr und Strafverfolgung als Grundlage der Erkenntnisgewinnung und Ermittlungsansatz ist es für eine effektive Aufgabenerfüllung unerlässlich, dass die Unterstützung der Polizeien auch die Veranlassung einer vorläufigen Sicherung dieser Daten umfasst, sofern und solange die Zuständigkeit einer Strafverfolgungs- oder Polizeibehörde noch nicht erkennbar ist. Das Bundeskriminalamt kann in diesem Fall vorläufig die Sicherung der Daten veranlassen, um zu ermöglichen, dass diese im weiteren Verlauf der Sachverhaltsbearbeitung durch die sachlich und örtlich zuständige Behörde vollständig erhoben werden können, das heißt sie trotz erkannter möglicher Relevanz nicht zwischenzeitlich durch die Telekommunikationsanbieter oder die betroffenen Personen selbst gelöscht werden.

Wie bei der Sicherungsanordnung zum Zwecke der Strafverfolgung ergibt sich der Bedarf für die Einführung der Sicherungsanordnung für das Bundeskriminalamt in Wahrnehmung seiner Aufgabe als Zentralstelle also aus dem Umstand, dass Verkehrsdaten flüchtig sind. Wie bereits zu Artikel 1 Nummer 2 dargelegt, speichern zum Beispiel die Netzbetreiber die Daten zu betrieblichen Zwecken häufig maximal sieben Tage lang, sofern überhaupt eine Speicherung erfolgt. Bei anderen Telekommunikationsunternehmen wie zum Beispiel E-Mail-Anbietern besteht die Möglichkeit, dass der Kunde seinen Account jederzeit selbst löscht, eine weitere Aufbewahrung der Daten ist dem Anbieter zu geschäftlichen Zwecken dann nicht erlaubt. Es besteht folglich das Risiko, dass die Daten nicht oder nicht mehr vorliegen, sobald sich die Zuständigkeit einer Strafverfolgungs- oder Polizeibehörde beziehungsweise gegebenenfalls des Bundeskriminalamtes selbst festgestellt ist und die Voraussetzung für deren Erhebung vorliegen, mit der Konsequenz, dass weitere Ermittlungen wegen des Fehlens von Daten aussichtslos sind. Diesem Risiko ist mit dem Instrument der Sicherungsanordnung für das Bundeskriminalamt als Zentralstelle entgegenzuwirken.

Die Erhebungsbefugnisse verbleiben bei den jeweils zuständigen Strafverfolgungs- und Polizeibehörden des Bundes und der Länder. Bis die Zuständigkeit geklärt ist und die Voraussetzungen für die etwaige Erhebung der

Verkehrsdaten vorliegen, soll ausdrücklich lediglich der Verlust der Daten durch die Sicherung verhindert werden. Eine Datenerhebungsbefugnis für die zu sichernden Daten wird dem Bundeskriminalamt in seiner Aufgabe als Zentralstelle nicht zugeschrieben.

### **Zu Absatz 1**

In Absatz 1 wird die Sicherungsanordnung für das Bundeskriminalamt zur Erfüllung der Aufgabe als Zentralstelle nach § 2 Absatz 1 geregelt.

Sofern und solange die Zuständigkeit einer Strafverfolgungs- oder Polizeibehörde noch nicht erkennbar bzw. festgestellt ist, wird das Bundeskriminalamt befugt, Verkehrsdaten für eine etwaige Erhebung nach § 100g Absatz 1 bis 4 der Strafprozessordnung (StPO), eine etwaige Erhebung nach den für die zuständigen Landespolizeibehörden geltenden Vorschriften oder eine etwaige Erhebung bei Feststellung der Zuständigkeit des Bundeskriminalamtes gemäß § 5 Absatz 1 Satz 1 beim Telekommunikationsunternehmen durch Anordnung zu sichern.

Das Bundeskriminalamt erhält in seiner Aufgabenwahrnehmung als Zentralstelle regelmäßig Hinweise auf Straftaten, bezüglich derer es die zuständige Strafverfolgungs- oder Polizeibehörde in Deutschland ermitteln muss. Dabei handelt es sich um Sachverhalte, die entweder der Gefahrenabwehr oder der Strafverfolgung zugeführt werden müssen. Sie stammen von ausländischen Sicherheitsbehörden, von nachrichtendienstlichen Behörden, entstehen durch eigene Recherchen im Rahmen der Unterstützung des Bundeskriminalamtes als Zentralstelle für die Kriminalpolizei die Polizeien des Bundes und der Länder bei der Verhütung, Aufklärung und Verfolgung von Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung oder werden dem Bundeskriminalamt von privaten Stellen, zum Beispiel Social Media Plattformen, gemeldet. Bis die Zuständigkeit geklärt ist, wird das Bundeskriminalamt befugt, die Sicherung der Verkehrsdaten, die für die weitere effektive und zielgerichtete gefahrenabwehrende oder strafverfolgende Sachbearbeitung von Bedeutung sein können, anzuordnen.

Hinsichtlich der Anforderungen zum Vorliegen von tatsächlichen Anhaltspunkten gemäß Absatz 1 Nummer 1 Buchstabe a, dass eine Straftat begangen worden ist, welche die Erhebung nach § 100g Absatz 1 bis 4 StPO rechtfertigen würde, wird auf die Begründung des Entwurfs eines Gesetzes zur Einführung einer IP-Adressspeicherung und Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren zur Änderung der Strafprozessordnung unter Nummer 2, zu § 100g Absatz 7 StPO, verwiesen.

Für die Sicherungsanordnung zur Gefahrenabwehr müssen gemäß Nummer 1 Buchstabe b tatsächliche Anhaltspunkte vorliegen, dass eine Person innerhalb eines überschaubaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Straftat von erheblicher Bedeutung, insbesondere eine in §100a Absatz 2 StPO bezeichnete Straftat, begehen wird. Steht diese Person mit einer anderen Person derart in Kontakt beziehungsweise Verbindung, dass eine Verwicklung der anderen Person in prognostizierte Straftat angenommen werden kann, kann nach Nummer 1 Buchstabe c auch in Bezug auf die andere Person eine Sicherungsanordnung erfolgen. In beiden Fällen soll entweder eine Erhebung durch die zuständigen Polizeibehörden nach den jeweils für sie geltenden Vorschriften oder, sofern eine Gefahrenlage im Sinne von § 5 Absatz 1 vorliegt, eine Erhebung durch das Bundeskriminalamt selbst nach § 52 Absatz 1 ermöglicht werden.

Von der Sicherungsanordnung zur Gefahrenabwehr wird damit zum einen die Person erfasst, bei der gestützt auf Tatsachen die Begehung einer Straftat von erheblicher Bedeutung prognostiziert wird. Zum anderen werden Personen erfasst, bei denen tatsächliche Anhaltspunkte für eine Beziehung zu einer solchen Person beziehungsweise für einen Tatbezug bestehen und damit Anhaltspunkte für eine Einbeziehung in den Handlungskomplex der Straftatenbegehung, insbesondere eine Verwicklung in den Hintergrund oder das Umfeld der prognostizierten Straftat, die abgewehrt beziehungsweise verhütet werden soll. Zum Zeitpunkt der Gefahrenprognose kann die für die Erhebung von Verkehrsdaten erforderliche konkrete Wahrscheinlichkeit des Eintretens der Gefahr in Bezug auf einen Störer gegebenenfalls bereits vorliegen, aufgrund der offenen Frage der Zuständigkeit einer Polizeibehörde ist eine unmittelbare Erhebung aber noch nicht möglich. Im Falle der Kontaktpersonen wiederum lassen Anhaltspunkte einen Zusammenhang zur Gefahr beziehungsweise den Gefährder oder Störer erkennen, die nach weiteren Ermittlungen den Gefahrenverdacht verdichten könnten, der eine Erhebung der Daten möglich machen würde.

Die Sicherungsanordnung darf gegenüber denjenigen angeordnet werden, die auch zur Herausgabe verpflichtet wären, also gegenüber allen Telekommunikationsanbietern, siehe näher bei der Begründung des Entwurfs eines Gesetzes zur Einführung einer IP-Adressspeicherung und Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren zur Änderung der Strafprozessordnung unter Nummer 2, zu § 100g Absatz 7 StPO.

Die Sicherung darf für den Fall einer etwaigen Erhebung angeordnet werden. Die gesicherten Daten dürfen ausschließlich für die korrespondierende Erhebungsmaßnahme verwendet werden, siehe näher bei der Begründung des Entwurfs eines Gesetzes zur Einführung einer IP-Adressspeicherung und Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren zur Änderung des Telekommunikationsgesetzes (TKG) unter Artikel 6 Nummer 2, zu § 175 Absatz 1.

Nach Nummer 2 muss in den Fällen von Nummer 1 Buchstabe a und b ein persönlicher oder räumlicher Bezug der betroffenen Person zur Tat bestehen, siehe näher bei der Begründung des Entwurfs eines Gesetzes zur Einführung einer IP-Adressspeicherung und Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren zur Änderung der Strafprozessordnung unter Nummer 2, zu § 100g Absatz 7 StPO. In den Fällen von Nummer 1 Buchstabe c kommt diese Voraussetzung bereits durch dessen Tatbestandsmerkmale zur Geltung.

Nach Nummer 3 müssen die Verkehrsdaten für die jeweiligen Zwecke der Erhebung von Bedeutung sein können. Es reicht aus, dass im Moment der Sicherungsanordnung die Möglichkeit besteht, dass die Verkehrsdaten für die etwaige Erhebung (Abwehr schwerwiegender Gefahren und die Verhütung gewichtiger Straftaten) verwendet werden können. Die erforderliche Prognosestellung, dass die Daten für die weitere Sachverhaltsaufklärung und vollständige Gefahrenräumung von Bedeutung sein müssen, stellt sicher, dass keine Daten gesichert werden, die mit dem Sachverhalt nicht unmittelbar in Verbindung gebracht werden können.

#### **Zu Absatz 2**

Die Vorschrift regelt die Anordnungscompetenz. Die zuständige Abteilungsleitung oder deren Vertretung kann die Anordnungsbefugnis auf Bedienstete des Bundeskriminalamtes mit Befähigung zum Richteramt übertragen.

#### **Zu Absatz 3**

Die Vorschrift regelt den Anordnungsinhalt. Anzugeben sind der Name und die Anschrift des Betroffenen, soweit dies möglich ist. Diese Einschränkung zielt auf Fälle, in denen die vollständigen Angaben zur Person des Betroffenen der Behörde nicht bekannt sind.

Da bei der Sicherung von in einer Funkzelle angefallenen Verkehrsdaten Informationen zu Rufnummer oder Kennung eines Mobiltelefons noch nicht vorliegen, genügt eine räumlich und zeitlich hinreichende Bezeichnung der Telekommunikation, sodass sämtliche Verkehrsdaten unter den Voraussetzungen des Absatzes 1 Satz 1 Nummer 1 oder Nummer 2 und Satz 2 gesichert werden können, die innerhalb einer Funkzelle anfallen oder angefallen sind.

Neben Art, Umfang und Dauer der Maßnahme unter Benennung des Endzeitpunktes sind die Art der zu erheben den Daten sowie deren voraussichtlich Bedeutung für die Zwecke der Erhebung zu benennen. Zudem muss die schriftliche Angabe der wesentlichen Gründe für die Anordnung der Maßnahme erfolgen.

#### **Zu Absatz 4**

Die Vorschrift regelt den Zeitraum der Anordnung. Die Sicherung darf für einen Zeitraum von höchstens drei Monaten angeordnet werden.

#### **Zu Absatz 5**

Die Vorschrift regelt die Mitwirkungspflichten und den Entschädigungsanspruch der Verpflichteten. In Bezug genommen werden die Regelungen des Telekommunikationsgesetzes und der Telekommunikations-Überwachungsverordnung. Der Umfang der Entschädigung bemisst sich nach § 23 und Anlage 3 des Justizvergütungs- und -entschädigungsgesetzes (JVEG).

#### **Zu Nummer 3 (§§ 39a, 39b)**

##### **Zu § 39a**

§ 39a regelt die Befugnis zum biometrischen Abgleich mit öffentlich zugänglichen Daten aus dem Internet zum Zweck der Abwehr von Gefahren des internationalen Terrorismus. Ziel der Maßnahme kann es unter anderem sein, Hinweise auf den Aufenthaltsort von aus dem Untergrund agierender Störer zu erhalten, um terroristische Taten zu verhindern. Ebenso können Querverbindungen zwischen Personen und Strukturen durch biometrische Übereinstimmungen ermittelt werden. Zudem können beispielsweise Akteure in Propagandavideos terroristischer Organisationen identifiziert werden.

Die Tätigkeit des Bundeskriminalamtes nach § 5 Absatz 1 Satz 2 unterfällt vollumfänglich dem Begriff der nationalen Sicherheit nach Artikel 4 Absatz 2 Satz 3 des Vertrags über die Europäische Union im Sinne der Definition des Europäischen Gerichtshofs (Urteil vom 6. Oktober 2020, Rechtssachen C-511/18, C-512/18 und C-520/18, Randnummer 135). Dem Bundeskriminalamt ist im Rahmen der Wahrnehmung der Aufgabe nach § 5 Absatz 1 Satz 2 die Aufgabe zugewiesen, terroristische Gefahren abzuwehren beziehungsweise terroristische Straftaten zu verhüten. Die in § 5 Absatz 1 Satz 2 einbezogenen Straftaten nach § 129a Absatz 1 und 2 des Strafgesetzbuchs setzen den Katalog der Richtlinie (EU) 2017/541 des Europäischen Parlaments und des Rates vom 15. März 2017 zur Terrorismusbekämpfung und zur Ersetzung des Rahmenbeschlusses 2002/475/JI des Rates und zur Änderung des Beschlusses 2005/671/JI des Rates um (zum Rahmenbeschluss 2002/475/JI: Bundestagsdrucksache 15/813, S. 6f.).

Das Bundesverfassungsgericht (BVerfG) führt zu der Vorgängerfassung von § 5 Absatz 1 Satz 2 aus: „Straftaten mit dem Gepräge des Terrorismus in diesem Sinne zielen auf eine Destabilisierung des Gemeinwesens und umfassen hierbei in rücksichtsloser Instrumentalisierung anderer Menschen Angriffe auf Leib und Leben beliebiger Dritter. Sie richten sich gegen die Grundpfeiler der verfassungsrechtlichen Ordnung und das Gemeinwesen als Ganzes.“ (BVerfG, Urteil vom 24. April 2016, Az. 1 BvR 966/09 u.a., Randnummer 96).

Im Übrigen wird auf die Begründung zu §§ 9a und 63b verwiesen.

#### **Zu § 39b**

§ 39b regelt die Befugnis zur automatisierten Datenanalyse zum Zweck der Abwehr von Gefahren des internationalen Terrorismus. Gerade im Phänomenbereich des internationalen Terrorismus, in dem die Täter häufig in dezentralen Strukturen operieren, ist das Erkennen von Zusammenhängen auf etwa gemeinsame Strukturen und Personengruppen von besonders hoher Bedeutung. Die technologischen Fähigkeiten des Bundeskriminalamtes müssen für diesen Bereich dem aktuellen Stand der Technik entsprechen.

Die fachliche Nutzung der nach § 39b Absatz 1 zum Zwecke der Analyse zusammengeführten Daten darf nur dann erfolgen, wenn die Voraussetzungen von Absatz 1 vorliegen, um den Einsatz einer jeweils angemessenen Eingriffsschwelle zu unterwerfen. Voraussetzung ist nach Satz 1 eine Gefahr im Zusammenhang mit Straftaten nach § 5 Absatz 1 Satz 2, soweit besonders gewichtige Rechtsgüter betroffen sind. Nach dem Urteil des Bundesverfassungsgerichts vom 16. Februar 2023 (Az. 1 BvR 1547/19, 1 BvR 2634/20) kann die automatisierte Datenanalyse ebenfalls bei einer hinreichend konkretisierten Gefahr für besonders gewichtigen Rechtsgütern erfolgen (Randnummer 105f.). Satz 2 Nummer 1 oder 2 entspricht der Rechtsprechung des Bundesverfassungsgerichts zu den Anforderungen an eine konkretisierte Gefahrenlage (Urteil vom 20. April 2016, Az. 1 BvR 966/09 und 1 BvR 1140/09, Randnummer 165). Auf Grund des Bezugs auf § 5 Absatz 1 Satz 2 ist in Absatz 1 Satz 2 Nummer 1 und 2 sichergestellt, dass der Einsatz der automatisierten Anwendung zur Datenanalyse auf den Schutz von besonders gewichtigen Rechtsgütern beschränkt ist. Für den Schutz von Sachen gilt entsprechend der Rechtsprechung des Bundesverfassungsgerichts ein enges Verständnis, nach dem etwa wesentliche Infrastruktureinrichtungen oder sonstige Anlagen mit unmittelbarer Bedeutung für das Gemeinwesen gefasst werden (BVerfG, Az. 1 BvR 1547/19, 1 BvR 2634/20, Randnummer 105).

Im Übrigen wird auf die Begründung zu §§ 9b und 63c verwiesen.

#### **Zu Nummer 4 (§ 52)**

##### **Zu Buchstabe a**

Die Vorschrift wird redaktionell angepasst, indem Anbieter öffentlich zugänglicher Telekommunikationsdienste als Verpflichtete benannt werden, ohne dass damit eine Änderung an der Rechtslage einhergeht.

##### **Zu Buchstabe b**

Auch im Rahmen der Wahrnehmung der Aufgabe des Bundeskriminalamtes zur Abwehr von Gefahren des internationalen Terrorismus gemäß § 5 Absatz 1 besteht der Bedarf, flüchtige Daten zu sichern, wenn die vorliegenden Erkenntnisse und Informationen noch keine hinreichend konkretisierte Zuordnung einzelner Gefährder oder Störer zulassen. Erforderlich ist eine weitere Verdichtung von Informationen, in deren Zuge sich Verdachtsmomente erhärten, Gefährder oder Störer identifiziert und Verbindungen zwischen Personen erhellt werden, die im Ergebnis eine Erhebung rechtfertigen könnten.

Zu Beginn der Gefahrermittlung kann es vorkommen, dass die Informationslage noch nicht ausreicht, um sie einem konkreten Gefährder oder Störer zuzuordnen. Zudem ist zumeist nicht eindeutig klar, welcher Natur die Beziehungen zu Kommunikationspartnern eines Störers sind. Erst wenn sich dies im Verlauf der Sachverhaltsaufklärung konkretisiert, ist eine Datenerhebung nach § 52 Absatz 1 zu den dort genannten Personen zulässig. Bis zu dem Zeitpunkt, in dem eindeutig festgestellt ist, dass zu der betroffenen Person eine Datenerhebung im Sinne der Nummer 1 bis Nummer 5 zulässig ist, soll sichergestellt sein, dass relevante Verkehrsdaten zum Beispiel zum E-Mail-Account der Person nicht gelöscht werden. Dies ist insbesondere dann von Bedeutung, wenn die Gefahr besteht, dass die betreffende Person selbst oder gar eine andere Person den Account vollständig löscht.

Das Gleiche gilt für ermittelte Telekommunikationsmittel der Personen im Umfeld des Störers (Sicherung noch gespeicherter Verkehrsdaten zu Mobilfunknummern) oder mögliche Aufenthalts- und Handlungsorte des Störers und seiner Kontaktpersonen (Sicherung hoch flüchtiger Funkzellendaten), bis festgestellt ist, ob zu ihnen eine Verkehrsdatenerhebung nach § 52 Absatz 1 angeordnet werden kann. Dann kann die zielgerichtete und vollständige Erhebung der Verkehrsdaten durch das Gericht erfolgen.

Darüber hinaus muss dem Umstand Rechnung getragen werden, dass bei Vorliegen der Voraussetzungen zur Erhebung von Verkehrsdaten nach § 52 Absatz 1 zeitgleich eine Sicherung der Verkehrsdaten angeordnet werden muss, um einen Datenverlust zu verhindern, bis die technischen Voraussetzungen zur unverzüglichen Erteilung der erforderlichen Auskünfte vorliegen. Vergleiche hierzu auch die Ausführungen zu Artikel 1 Nummer 2 zu § 100g Absatz 7 StPO des Entwurfs eines Gesetzes zur Einführung einer IP-Adressspeicherung und Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren.

Die Verkehrsdaten müssen für die jeweiligen Zwecke der Erhebung von Bedeutung sein können. Es reicht aus, dass im Moment der Sicherungsanordnung die Möglichkeit besteht, dass die Verkehrsdaten für die etwaige Erhebung (Abwehr schwerwiegender Gefahren und die Verhütung gewichtiger Straftaten) verwendet werden können. Die erforderliche Prognosestellung, dass die Daten für die weitere Sachverhaltsaufklärung und vollständige Gefahrenräumung von Bedeutung sein müssen, stellt sicher, dass keine Daten gesichert werden, die mit dem Sachverhalt nicht unmittelbar in Verbindung gebracht werden können.

#### **Zu Buchstabe c**

Es erfolgt eine redaktionelle Anpassung, indem die Verpflichteten benannt werden, ohne dass sich daraus eine Änderung der geltenden Rechtslage ergibt.

#### **Zu Buchstabe d**

##### **Zu Absatz 5**

Die Vorschrift regelt die Anordnungscompetenz. Die zuständige Abteilungsleitung oder deren Vertretung kann die Anordnungsbefugnis auf Bedienstete des Bundeskriminalamtes mit Befähigung zum Richteramt übertragen.

##### **Zu Absatz 6**

Die Vorschrift regelt den Anordnungsinhalt. Anzugeben sind der Name und die Anschrift des Betroffenen, soweit dies möglich ist. Diese Einschränkung zielt auf Fälle, in denen die vollständigen Angaben zur Person des Betroffenen der Behörde nicht bekannt sind.

Da bei der Sicherung von in einer Funkzelle angefallenen Verkehrsdaten Informationen zu Rufnummer oder Kennung eines Mobiltelefons noch nicht vorliegen, genügt eine räumlich und zeitlich hinreichende Bezeichnung der Telekommunikation, sodass sämtliche Verkehrsdaten gesichert werden, die innerhalb einer Funkzelle anfallen oder angefallen sind.

Neben Art, Umfang und Dauer der Maßnahme unter Benennung des Endzeitpunktes sind die Art der zu erheben den Daten sowie deren voraussichtlich Bedeutung für die Zwecke der Erhebung zu benennen. Zudem muss die schriftliche Angabe der wesentlichen Gründe für die Anordnung der Maßnahme erfolgen.

##### **Zu Absatz 7**

Die Sicherung darf für einen Zeitraum von höchstens drei Monaten angeordnet werden. Eine Verlängerung ist einmalig um höchstens drei Monate möglich, kann aber nur auf Antrag der zuständigen Abteilungsleitung oder deren Vertretung durch das Gericht angeordnet werden.

**Zu Absatz 8**

Die Vorschrift regelt die Mitwirkungspflichten und den Entschädigungsanspruch der Verpflichteten. Die Telekommunikationsunternehmen werden verpflichtet die Verkehrsdaten unverzüglich und vollständig zu sichern. In Bezug genommen werden zudem die Regelungen des Telekommunikationsgesetzes und der Telekommunikations-Überwachungsverordnung. Für die Entschädigung der Diensteanbieter sind die Regelung in § 23 JVEG entsprechend anwendbar.

**Zu Nummer 5 (§ 87a)**

Zur Sicherstellung der praktischen Wirksamkeit der § 10b Absatz 5 Satz 1 oder § 52 Absatz 8 Satz 1 sind die Regelungen, die eine unverzügliche und vollständige Sicherung der Daten durch die betroffenen Telekommunikationsunternehmen vorsehen, mit einem Bußgeld zu bewehren. Dabei werden sowohl vorsätzliche als auch fahrlässige Verstöße sanktioniert, um im Gleichlauf zum Elektronische-Beweismittel-Umsetzungs- und Durchführungsgesetz (EBewMG) bzw. zur Verordnung (EU) 2023/1543 sämtliche Begehungsformen zu berücksichtigen und die Umstände der Begehung einfließen zu lassen.

Für die Umsetzung der Sicherungsanordnung gelten die entsprechenden Vorgaben der Telekommunikations-Überwachungsverordnung (TKÜV) sowie der Technischen Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation, Erteilung von Auskünften (TR TKÜV) gemäß § 170 Absatz 5 Nummer 1a und Absatz 6 TKG. Dies gilt auch für die Sicherstellung der unverzüglichen Entgegennahme und Umsetzung von Anordnungen innerhalb und außerhalb der üblichen Geschäftszeiten gemäß § 12 TKÜV.

Geregelt werden der Bußgeldtatbestand und die zugehörige Bußgeldhöhe. Im Übrigen gelten die Vorschriften des Gesetzes über Ordnungswidrigkeiten (OWiG).

Die Obergrenze des zu verhängenden Bußgeldes bestimmt sich nach der Art der Zuwiderhandlung und dem Unrechtsgehalt. Unter wertender Heranziehung der Bußgeldhöhe bei Verstößen gegen die Pflicht der unverzüglichen Sicherung von angeforderten Daten nach Erhalt eines EPOC-PR gemäß Artikel 11 Absatz 1 der Verordnung (EU) 2023/1543 sollen die Fälle des Absatzes 1 mit einer Geldbuße bis zu fünfhunderttausend Euro geahndet werden können.

Die Fälle von Absatz 1 betreffen jeweils Verstöße gegen die grundlegenden Verpflichtungen im Zusammenhang mit der Ausführung von Sicherungsanordnungen nach § 10b Absatz 5 Satz 1 oder § 52 Absatz 8 Satz 1. Für die Verletzung dieser grundlegenden Handlungspflichten ist das Höchstmaß des Bußgeldrahmens angemessen. Die reibungslose Kooperation der Verpflichteten ist unerlässlich, um einen unwiederbringlichen Beweismittelverlust zu verhindern und insbesondere schwere Formen der Kriminalität zu bekämpfen. Der gewählte Sanktionsrahmen entfaltet die notwendige und effektiv abschreckende Wirkung.

**Zu Artikel 2 (Inkrafttreten)**

Die Bestimmung regelt das Inkrafttreten des Gesetzes.

**Stellungnahme des Nationalen Normenkontrollrates (NKR) gem. § 6 Abs. 1 NKR-G****Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit (NKR-Nr. 7733, BMI); Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse zur Abwehr von Gefahren des internationalen Terrorismus (NKR-Nr. 7734, BMI)**

Der Nationale Normenkontrollrat hat die Regelungsentwürfe mit folgendem Ergebnis geprüft:

**I Zusammenfassung**

<b>Bürgerinnen und Bürger</b>	keine Auswirkungen
<b>Wirtschaft</b>	keine Auswirkungen
<b>Verwaltung</b>	nicht dargestellt
<b>„One in, one out“-Regel</b>	nicht dargestellt
<b>Evaluierung</b>	nicht vorgesehen
<b>Nutzen des Vorhabens</b>	Das Ressort hat keinen Nutzen dargestellt.
<b>Digitaltauglichkeit (Digitalcheck)</b>	Das Ressort hat Möglichkeiten zum digitalen Vollzug der Neuregelung (Digitaltauglichkeit) geprüft und hierzu einen Digitalcheck durchgeführt.

**Regelungsfolgen**

Der Nationale Normenkontrollrat (NKR) hat im Rahmen seines gesetzlichen Auftrags zu beanstanden, dass die Regelungsfolgen nicht methodengerecht dargestellt sind. So hat das Ressort die einmaligen und laufenden Kosten der Bundesverwaltung für die Schaffung und Wartung der technischen Infrastruktur entgegen der ressortverbindlichen Methodik nicht unter E „Erfüllungsaufwand“, sondern lediglich unter D „Haushaltsausgaben“ dargestellt. Der NKR beanstandet, dass durch diese nicht sachgemäße Einordnung von Folgekosten als „Haushaltsausgaben“ Aufwände der Erfüllungsaufwands-Bilanz der Bundesregierung entzogen werden. Aus diesem Grund wird er die Aufwände, anders als vom Ressort dargestellt, methodengerecht als Erfüllungsaufwand bilanzieren.

**Digitaltauglichkeit**

Das Ressort hat Möglichkeiten zum digitalen Vollzug der Neuregelung (Digitaltauglichkeit) geprüft und dazu einen Digitalcheck vorgelegt. Der NKR empfiehlt - unabhängig vom Schwellenwert für Erfüllungsaufwand - eine zeitnahe Evaluierung, auch aufgrund der besonderen politischen Bedeutung des Vorhabens und Hinweise von Verbänden auf das Prinzip Datenschutz und Informationssicherheit.

## **II Regelungsvorhaben**

Mit den zwei Regelungsvorhaben (zustimmungsfrei/zustimmungspflichtig) sollen insbesondere die Rechtsgrundlagen geschaffen werden, um dem Bundeskriminalamt (BKA) und der Bundespolizei (BPol) die automatisierte Datenanalyse (auch mit Künstlicher Intelligenz) für den biometrischen Internetabgleich, insbesondere von Bildern sowie das Testen und Trainieren von IT-Produkten, zu ermöglichen. Auch das Bundesamt für Migration und Flüchtlinge (BAMF) soll zu Identifizierungszwecken die Möglichkeit zum biometrischen Abgleich von Lichtbildern mit öffentlich zugänglichen Daten aus dem Internet erhalten.

## **III Bewertung**

### **III.1 Erfüllungsaufwand**

#### **Bürgerinnen und Bürger**

Das Regelungsvorhaben führt nicht zu zusätzlichen Kostenbelastungen für die Bürgerinnen und Bürger.

#### **Wirtschaft**

Es fällt kein Erfüllungsaufwand für die Wirtschaft an.

#### **Verwaltung**

Der Bundesverwaltung entstehen nach Angaben des Ressorts einmalige und jährliche Kosten für den Aufbau und die Entwicklung einer technischen Umgebung für die automatische Datenanalyse. Weiterhin entstehen dem BKA und der BPol jährliche Aufwände sowohl für die technische Infrastruktur samt Lizenz-, Betriebs-, Wartungs- und Pflegekosten als auch für Personal. Insgesamt geht das Ressort von einmaligen Kosten in Höhe von rund 40,7 Mio. Euro und jährlichen Aufwänden von rund 44 Mio. Euro aus. Gleichzeitig nimmt das Ressort an, dass die jährlichen Kosten durch Synergieeffekte im Rahmen des IT-Entwicklungs-Programms P20 um rund jährlich 15 Mio. Euro gesenkt werden können.

Das Ressort weist diese Aufwände lediglich unter D „Haushaltsausgaben ohne Erfüllungsaufwand“ aus, nicht indes unter E „Erfüllungsaufwand“. Dies entspricht nicht dem verbindlichen

Erfüllungsaufwandsleitfaden, nach welchem diese Aufwände eindeutig Erfüllungsaufwand darstellen. Die Darstellung ist somit nicht methodengerecht. Zudem fehlt eine summarische Darstellung der jährlichen Kosten.

### III.2 „One in, one out“

Die „One in, one out“-Regel der Bundesregierung findet auf den Erfüllungsaufwand Anwendung. Dadurch, dass kein Erfüllungsaufwand dargestellt wurde, enthält der Entwurf – entgegen der Beschlusslage der Bundesregierung – keine Angaben zu der „One in, one out“-Regel.

### III.3 Evaluierung

Der Entwurf sieht – entgegen der Beschlusslage der Bundesregierung – keine Evaluierung vor. Weil das Ressort keinen Erfüllungsaufwand ausweist, greift nicht die grundsätzliche Evaluierungspflicht anhand des Schwellenwerts von 5 Mio. Euro jährlichen Erfüllungsaufwands. Das Ressort gibt zudem an, dass mit dem Vorhaben an bestehende Aufgaben der Behörden angeknüpft werde und diese insbesondere durch die parlamentarische Kontrolle sowie der Fach- und Rechtsaufsicht sowie bestehender Berichtspflichten und gerichtlicher Rechtsschutzmöglichkeiten kontrolliert würden.

Der NKR empfiehlt - unabhängig vom Schwellenwert für Erfüllungsaufwand - eine zeitnahe Evaluierung, auch aufgrund der besonderen politischen Bedeutung des Vorhabens und Hinweisen von Verbänden auf das Prinzip Datenschutz und Informationssicherheit.

24. April 2026

Lutz Goebel  
*Vorsitzender*

Prof. Dr. Sabine Kuhlmann  
*Berichterstatterin für das  
Bundesministerium des Innern*

Vorabfassung – wird durch die lektorierte Fassung ersetzt.

Anlage 3

**Stellungnahme der Bundesregierung zur Stellungnahme des Nationalen Normenkontrollrats**

Die Bundesregierung nimmt zur Stellungnahme des Nationalen Normenkontrollrats (NKR) vom 24. April 2026 wie folgt Stellung:

Der NKR beanstandet wie folgt:

1. Die Darstellung der Regelungsfolgen erfolge nicht methodengerecht. Die Mehrbedarfe würden entgegen der ressortverbindlichen Methodik nicht unter E „Erfüllungsaufwand“, sondern unter D „Haushaltsausgaben“ dargestellt. Dadurch würden die Mehrbedarfe der Erfüllungsaufwands-Bilanz der Bundesregierung entzogen.

Stellungnahme der Bundesregierung:

Die Darstellung der Mehrbedarfe erfolgt im Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit. Es wird auf die Stellungnahme der Bundesregierung zur Stellungnahme des NKR (NKR-Nr. 7733) verwiesen.

2. Der Entwurf sei zu evaluieren. Dies gelte unabhängig vom Schwellenwert für den Erfüllungsaufwand aufgrund der besonderen politischen Bedeutung des Vorhabens und Hinweisen von Verbänden auf das Prinzip Datenschutz und Informationssicherheit.

Stellungnahme der Bundesregierung:

Die Bundesregierung hat in der Begründung des Gesetzentwurfs ausgeführt, dass eine Evaluierung nicht erforderlich ist. Daran hält die Bundesregierung fest. Die neuen Regelungen knüpfen an den bestehenden gesetzlichen Aufgaben des Bundeskriminalamts an. Die Anwendung der Befugnisse sowie deren Auswirkung unterliegt einer kontinuierlichen Kontrolle, insbesondere durch die parlamentarische Kontrolle, die Fach- und Rechtsaufsicht sowie die bestehenden Berichtspflichten und gerichtliche Rechtsschutzmöglichkeiten.

Vorabfassung – wird durch die lektorierte Fassung ersetzt.