Deutscher Bundestag **Drucksache 20/14704**

20. Wahlperiode 28.01.2025

Gesetzentwurf

der Fraktionen SPD und BÜNDNIS 90/DIE GRÜNEN

Entwurf eines Gesetzes zur Stärkung der polizeilichen Befugnisse

A. Problem und Ziel

Dieser Gesetzentwurf dient insbesondere der Stärkung digitaler Befugnisse der Sicherheitsbehörden.

Die Messerattacke von Aschaffenburg am 22. Januar 2025, der Anschlag auf den Weihnachtsmarkt in Magdeburg am 22. Dezember 2024 und der islamistische Anschlag am 23. August 2024 auf einem Volksfest in Solingen haben deutlich gemacht, dass sich die Sicherheits- und Bedrohungslage in Deutschland erheblich verschärft hat. Auch vor diesem Hintergrund sollen mit dem vorgelegten Gesetzentwurf die Befugnisse der Sicherheitsbehörden bei Gefahrenabwehr und Strafverfolgung gestärkt werden.

Erfolgreiche Polizeiarbeit erfordert moderne und sachgerechte polizeiliche Befugnisse. Dies betrifft angesichts der aktuellen Herausforderungen zunehmend die digitale Welt. Bundeskriminalamt und Bundespolizei benötigen vor diesem Hintergrund Zugriff auf die erforderlichen Daten und müssen über die notwendigen Instrumente verfügen, Daten aufzubereiten und auszuwerten. Der Gesetzentwurf verfolgt das Ziel, das Bundeskriminalamt bei der Erfüllung der Aufgaben als Zentralstelle der deutschen Polizeibehörden und dem Schutz von Verfassungsorganen sowie die Bundespolizei – insbesondere beim Grenzschutz – mit zeitgemäßen Befugnissen auszustatten.

Zudem soll für alle Strafverfolgungsbehörden eine ausdrückliche Ermächtigungsgrundlage geschaffen werden, die den Abgleich von öffentlich zugänglichen Daten aus dem Internet mit Lichtbildern und Stimmen von Tatverdächtigen und anderen gesuchten Personen auf eine rechtssichere Grundlage stellt.

Waffenverbotszonen und Allgemeinverfügungen, die das Mitführen von Waffen und gefährlichen Gegenständen verbieten, können nur eine Wirkung entfalten, wenn sie durchgesetzt werden. Hierzu bedarf es neuer Befugnisse für die Bundespolizei zur Kontrolle von Personen auf dem Gebiet der Eisenbahnen des Bundes, wenn dort das Mitführen von Waffen oder gefährlichen Gegenständen untersagt ist.

B. Lösung

Für den biometrischen Internetabgleich, die automatisierte Datenanalyse, BKA-Anfragen bei Banken sowie Waffenverbotszonen sollen neue Befugnisse geschaffen werden:

Die Befugnis zum biometrischen Abgleich von öffentlich zugänglichen Daten aus dem Internet dient dem Zweck, dass die Strafverfolgungsbehörden zu Strafverfolgungszwecken sowie darüber hinaus das Bundeskriminalamt und die Bundespolizei für weitere (polizeiliche Aufgaben) biometrische Daten zu Gesichtern und Stimmen mittels automatisierter technischer Verfahren mit Internetdaten (z. B. soziale Medien), abgleichen können. Ziel ist es insbesondere, Tatverdächtige zu identifizieren und zu lokalisieren.

Digitalisierung führt dazu, dass Datenmengen grundsätzlich ansteigen und weiter ansteigen werden, sowie zunehmend große Datenmengen aufbereitet und ausgewertet werden müssen. Hierfür sollen Befugnisse zur automatisierten Datenanalyse für Bundeskriminalamt und Bundespolizei geschaffen werden. Diese Befugnisse können dazu dienen, bei großen Datenmengen, Verbindungen/Beziehungen zwischen Informationen herzustellen. Die Polizeibehörden werden auf diese Weise in die Lage versetzt, bereits im polizeilichen Informationssystem oder im polizeilichen Informationsverbund vorhandene Informationen besser, schneller und effizienter auszuwerten. Damit entsprechende IT- und KI-Systeme auch ordnungsgemäß getestet und trainiert werden, bedarf es zur Rechtssicherheit einer entsprechenden Rechtsgrundlage.

Bei Ermittlungen des Bundeskriminalamts kann es erforderlich sein, polizeiliche Anfragen an geldwäscherechtlich Verpflichtete wie z. B. Banken zu stellen. Damit Banken in der Folge nicht das Konto der betroffenen Person kündigen, ist eine Vorschrift im Gesetzentwurf enthalten, die den Banken bei der Kontofortführung Rechtssicherheit gibt. Damit soll eine verfrühte Unterrichtung der Betroffenen – und damit mögliche Beeinträchtigung der Polizeiarbeit – vermieden werden.

Gegenstand ist ebenfalls eine Befugnis, die anlassbezogen im Falle der Anordnung von Waffenverbotszonen oder im Geltungsbereich von Allgemeinverfügungen der Bundespolizei die stichprobenartige Befragung, Identitätskontrolle sowie Durchsuchung von Personen erlaubt, die die Waffenverbotszone betreten möchten oder sich darin befinden.

C. Alternativen

Keine.

D. Haushaltsausgaben ohne Erfüllungsaufwand

Es entstehen keine Haushaltsausgaben ohne Erfüllungsaufwand.

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 Softwarebeschaffung bzw. -entwicklung und -betrieb entstehen Aufwände, ferner weitere sächliche und personelle Aufwände, die in den Folgejahren aufwachsend sein werden, sich derzeit aber insgesamt noch nicht beziffern lassen. Die Aufwände entstehen beim Bundeskriminalamt, bei der Bundespolizei sowie bei den Strafverfolgungsbehörden.

F. Weitere Kosten

Es entstehen keine weiteren Kosten.

Entwurf eines Gesetzes zur Stärkung der polizeilichen Befugnisse

Vom ...

Der Bundestag hat 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 Artikel 5 des Gesetzes vom 30. Juli 2024 (BGBl. 2024 I Nr. 255) geändert worden ist, wird wie folgt geändert:

1. Die Inhaltsübersicht wird wie folgt geändert:
   a) Nach der Angabe zu § 10a wird folgende Angabe eingefügt:
      „§ 10b Nachträglicher biometrischer Abgleich mit allgemein öffentlich zugänglichen Daten aus dem Internet; Verordnungsermächtigung“.
   b) Nach der Angabe zu § 16 wird folgende Angabe eingefügt:
      „§ 16a Automatisierte Datenanalyse; Verordnungsermächtigung“.
   c) Die Angabe zu § 22 wird wie folgt gefasst:
      „§ 22 Weiterverarbeitung von Daten zu weiteren Zwecken; Verordnungsermächtigung“.
   d) Nach der Angabe zu § 63a wird folgende Angabe eingefügt:
      „§ 63b Nachträglicher biometrischer Abgleich mit allgemein öffentlich zugänglichen Daten aus dem Internet; Verordnungsermächtigung“.
2. Dem § 9 wird folgender Absatz 7 angefügt:

   „(7) Soweit sich die Erhebung personenbezogener Daten nach Absatz 1 oder 2 an Verpflichtete nach § 2 Absatz 1 des Geldwäschegesetzes richtet und auf eine schwere Straftat nach § 100a Absatz 2 der Strafprozessordnung bezieht, kann das Bundeskriminalamt den Verpflichteten anweisen, für einen vom Bundeskriminalamt vorab bestimmten Zeitraum, der sechs Monate nicht überschreiten darf, nicht allein auf Grund der Erhebung personenbezogener Daten durch das Bundeskriminalamt einseitige Handlungen vorzunehmen, die für den Betroffenen nachteilig sind und die über die Erteilung der Auskunft hinausgehen, insbesondere bestehende Verträge oder Geschäftsverbindungen zu beenden, ihren Umfang zu beschränken oder ein Entgelt zu erheben oder zu erhöhen. Soweit eine Anweisung nach Satz 1 ergeht, ist diese mit dem ausdrücklichen Hinweis zu verbinden, dass das Auskunftsersuchen nicht die Aussage beinhaltet, dass sich die betroffene Person rechtswidrig verhalten hat oder ein darauf gerichteter Verdacht bestehen müsse. Die Verpflichteten nach § 2 Absatz 1 des Geldwäschegesetzes dürfen für das Befolgen einer Anweisung nach Satz 1 nicht nach zivilrechtlichen, strafrechtlichen oder aufsichtsrechtlichen Vorschriften verantwortlich gemacht oder disziplinarrechtlich verfolgt werden.“
3. Nach § 10a wird folgender § 10b eingefügt:

„§ 10b

Nachträglicher biometrischer Abgleich mit allgemein öffentlich zugänglichen Daten aus dem Internet; Verordnungsermächtigung

(1) Das Bundeskriminalamt kann zur Ergänzung vorhandener Sachverhalte biometrische Daten zu Gesichtern und Stimmen, auf die es zur Erfüllung seiner Aufgaben zugreifen darf, mit allgemein öffentlich zugänglichen personenbezogenen Daten aus dem Internet mittels einer automatisierten Anwendung zur Datenverarbeitung biometrisch abgleichen, sofern

1. dies im Rahmen der Erfüllung seiner Aufgabe als Zentralstelle nach § 2 Absatz 2 Nummer 1 zur Identifizierung oder Ermittlung des Aufenthaltsorts der Zielperson erforderlich ist,
2. bestimmte Tatsachen den Verdacht begründen, dass eine Straftat im Sinne des § 100b Absatz 2 der Strafprozessordnung begangen worden ist oder die Annahme rechtfertigen, dass eine Person innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine solche Straftat begehen wird, und
3. die Verfolgung oder Verhütung der Straftat auf andere Weise aussichtslos oder wesentlich erschwert wäre.

Ein Abgleich mit Daten nach Satz 1 aus im Internet allgemein öffentlich zugänglichen in Echtzeit erhobenen Daten ist ausgeschlossen.

(2) Die Maßnahme nach Absatz 1 Satz 1 darf gegen die in § 18 Absatz 1 sowie § 19 Absatz 1 Satz 1 Nummer 2 bezeichneten Personen durchgeführt werden. Bezüglich einer Person nach § 19 Absatz 1 Satz 1 Nummer 2 ist die Maßnahme unzulässig, wenn überwiegende schutzwürdige Interessen der betreffenden Person entgegenstehen.

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

(4) Maßnahmen nach Absatz 1 Satz 1 dürfen 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 auch durch die Präsidentin oder den Präsidenten des Bundeskriminalamtes oder ihrer oder seiner Vertretung getroffen werden. Sofern die Anordnung der Präsidentin oder des Präsidenten des Bundeskriminalamtes oder ihrer oder seiner Vertretung nicht binnen drei Tagen von dem Gericht bestätigt wird, tritt sie außer Kraft. Die Anordnung ergeht schriftlich. In ihrer Entscheidungsformel sind anzugeben:

1. die Person, zu deren Identifizierung oder Aufenthaltsermittlung die Maßnahme angeordnet wird,
2. die biometrischen Daten aus dem Strafverfahren oder dem Vorgang, die dieser Person zuzuordnen sind und die zum Abgleich herangezogen werden sollen,
3. der Tatvorwurf oder Sachverhalt, auf Grund dessen die Maßnahme angeordnet wird, und
4. die eingesetzte automatisierte Anwendung zur Datenverarbeitung.

(5) In der Begründung der Anordnung sind die Voraussetzungen für die Maßnahme nach Absatz 1 Satz 1 und die wesentlichen Abwägungsgesichtspunkte darzulegen. Insbesondere sind einzelfallbezogen die bestimmten Tatsachen, die den Verdacht begründen, die wesentlichen Erwägungen zur Erforderlichkeit und Verhältnismäßigkeit der Maßnahme, die wesentlichen Einzelheiten zur technischen Funktionsweise der automatisierten Anwendung zur Datenverarbeitung sowie die Subsidiarität zu anderen Maßnahmen anzugeben.

(6) Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch eine Maßnahme nach Absatz 1 Satz 1 allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt werden, ist die Maßnahme unzulässig. Erkenntnisse aus dem Kernbereich privater Lebensgestaltung, die durch eine Maßnahme nach Absatz 1 Satz 1 erlangt wurden, dürfen nicht verwertet werden. Aufzeichnungen über solche Erkenntnisse sind unverzüglich zu löschen. Die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren. Bei

Maßnahmen nach Absatz 1 Satz 1 ist, soweit möglich, technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. Erkenntnisse, die durch Maßnahmen nach Absatz 1 Satz 1 erlangt wurden und den Kernbereich privater Lebensgestaltung betreffen, sind unverzüglich zu löschen oder von der Präsidentin oder dem Präsidenten des Bundeskriminalamtes oder ihrer oder seiner Vertretung dem anordnenden Gericht zur Entscheidung über die Verwertbarkeit und Löschung der Daten vorzulegen. Die Entscheidung des Gerichts über die Verwertbarkeit ist für das weitere Verfahren bindend.

(7) Die im Rahmen des Abgleichs nach Absatz 1 Satz 1 erhobenen Daten sind nach Durchführung des Abgleichs unverzüglich zu löschen, sofern sie keinen konkreten Ermittlungsansatz für den Ausgangssachverhalt aufweisen. Die Weiterverarbeitung der beim Abgleich erhobenen Daten ist im Übrigen unzulässig.

(8) Bei jeder Maßnahme nach Absatz 1 Satz 1 ist die Bezeichnung der eingesetzten automatisierten Anwendung zur Datenverarbeitung, der Zeitpunkt ihres Einsatzes sowie die Organisationseinheit einschließlich einer individuellen Kennung der Person, die die Maßnahme durchführt, zu protokollieren. Nach Beendigung einer Maßnahme nach Absatz 1 Satz 1 ist die Stelle zu unterrichten, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz bei öffentlichen Stellen zuständig ist.

(9) Soweit zur Durchführung des Abgleichs nach Absatz 1 Satz 1 Dritte im Wege der Auftragsverarbeitung für das Bundeskriminalamt tätig werden, müssen diese ihren Sitz in der Europäischen Union oder einem Schengen-assoziierten Staat haben. Die Übermittlung personenbezogener Daten zur Durchführung der Maßnahme nach Absatz 1 Satz 1 ist nur innerhalb der Europäischen Union, einschließlich der Schengen-assoziierten Staaten, zulässig. Die Weiterverarbeitung durch Dritte von personenbezogenen Daten, die aus in § 12 Absatz 3 genannten Maßnahmen erlangt wurden, ist ausgeschlossen. Personenbezogene Daten werden nur an solche Personen übermittelt, die Amtsträger oder für den öffentlichen Dienst besonders Verpflichtete sind oder die zur Geheimhaltung verpflichtet worden sind. § 1 Absatz 2, 3 und 4 Nummer 1 des Verpflichtungsgesetzes ist auf die Verpflichtung zur Geheimhaltung entsprechend anzuwenden. Durch organisatorische und technische Maßnahmen ist zu gewährleisten, dass die Daten gegen unbefugte Kenntnisnahme geschützt sind.

(10) Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit führt Kontrollen bezüglich der Datenverarbeitung der Maßnahme nach Absatz 1 Satz 1 mindestens alle zwei Jahre durch.

(11) Die Bundesregierung bestimmt vor dem Einsatz von Maßnahmen nach Absatz 1 Satz 1 durch Rechtsverordnung ohne Zustimmung des Bundesrates nach Anhörung der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit das Nähere zu dem technischen Verfahren, den Sicherungsmaßnahmen zur Verhinderung unbefugter Datenzugriffe und, soweit eine Speicherung der abzugleichenden, öffentlich zugänglichen Lichtbild- Video- und Audiodateien für die Durchführung von Maßnahmen nach Absatz 1 technisch erforderlich ist, nähere Vorgaben zu Art, Umfang und Dauer. In der Rechtsverordnung nach Satz 1 bestimmt sie insbesondere

1. Eingabe- und Zugangsberechtigung,
2. Speicher- und Löschfristen,
3. Art der zu speichernden Daten,
4. Personenkreis, der von der Speicherung betroffen ist,
5. Dauer der Speicherung,
6. Protokollierung.“

4. Nach § 16 wird folgender § 16a eingefügt:

„§ 16a

Automatisierte Datenanalyse; Verordnungsermächtigung

(1) Das Bundeskriminalamt kann zur Erfüllung der Aufgabe als Zentralstelle im Informationssystem oder im polizeilichen Informationsverbund gespeicherte personenbezogene Daten mittels einer automatisierten Anwendung zur Datenverarbeitung zusammenführen und darüber hinaus zum Zwecke der Analyse weiterverarbeiten, sofern bestimmte Tatsachen die Annahme rechtfertigen, dass eine Person innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Straftat im Sinne des § 100b Absatz 2 der Strafprozessordnung begehen wird oder begangen hat, diese auch im Einzelfall besonders schwer wiegt, und dies zur Verhütung oder Verfolgung der Straftat erforderlich ist.

(2) Das Bundeskriminalamt kann im Informationssystem oder im polizeilichen Informationsverbund gespeicherte personenbezogene Daten 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 Leib, Leben oder Freiheit einer nach § 6 zu schützenden Person 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 von auch im Einzelfall erheblicher Bedeutung gegen Leib, Leben oder Freiheit einer nach § 6 zu schützenden Person begehen wird, oder
2. das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums eine Straftat von auch im Einzelfall erheblicher Bedeutung gegen Leib, Leben oder Freiheit einer nach § 6 zu schützenden Person begehen wird,

und dies zur Verhütung dieser Straftat erforderlich ist.

(3) Im Rahmen der Weiterverarbeitung nach den Absätzen 1 und 2 können insbesondere datei- und informationssystemübergreifend Beziehungen oder Zusammenhänge zwischen Personen, Personengruppierungen, Institutionen, Organisationen, Objekten und Sachen hergestellt, unbedeutende Informationen und Erkenntnisse ausgeschlossen, Suchkriterien gewichtet, die eingehenden Erkenntnisse zu bekannten Sachverhalten zugeordnet sowie gespeicherte Daten statistisch ausgewertet werden. Für die Weiterverarbeitung von personenbezogenen Daten, die durch einen verdeckten Einsatz technischer Mittel in oder aus Wohnungen oder einen verdeckten Eingriff in informationstechnische Systeme erlangt wurden, gilt § 12 Absatz 3.

(4) Beim Einsatz selbstlernender Systeme ist sicherzustellen, dass diskriminierende Algorithmen weder herausgebildet noch verwendet werden. Soweit technisch möglich, muss die Nachvollziehbarkeit des verwendeten Verfahrens sichergestellt werden.

(5) Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit führt Kontrollen bezüglich der Datenverarbeitung der Maßnahme nach Absatz 1 mindestens alle zwei Jahre durch.

(6) Die Bundesregierung bestimmt vor dem Einsatz von Maßnahmen nach den Absätzen 1 und 2 durch Rechtsverordnung ohne Zustimmung des Bundesrates nach Anhörung der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit das Nähere zu dem technischen Verfahren, den Sicherungsmaßnahmen zur Verhinderung unbefugter Datenzugriffe und nähere Vorgaben zu Art und Umfang der verarbeiteten Daten. In der Rechtsverordnung nach Satz 1 bestimmt sie insbesondere

1. Eingabe- und Zugangsberechtigung,
2. Art der zu verarbeitenden Daten,
3. Personenkreis, der von der Verarbeitung betroffen ist,
4. besondere Regelungen über die Verarbeitung von Daten, die durch besonders eingriffsintensive Maßnahmen erhoben wurden,
5. Protokollierung, einschließlich einer individuellen Kennung der handelnden Personen.“

5. § 22 wird wie folgt geändert:

a) Die Überschrift wird wie folgt gefasst:

„ § 22

Weiterverarbeitung von Daten zu weiteren Zwecken; Verordnungsermächtigung“.

b) Die folgenden Absätze 3 und 4 werden angefügt:

„(3) Das Bundeskriminalamt darf zur Entwicklung, Überprüfung, Änderung oder zum Trainieren von IT-Produkten bei ihm vorhandene personenbezogene Daten weiterverarbeiten und an Dritte übermitteln, soweit dies erforderlich ist, weil

1. unveränderte Daten benötigt werden oder
2. eine Anonymisierung oder Pseudonymisierung der Daten nicht oder nur mit unverhältnismäßigem Aufwand möglich ist.

Es hat dabei sicherzustellen, dass diskriminierende Algorithmen weder herausgebildet noch verwendet werden. Soweit wie technisch möglich muss die Nachvollziehbarkeit des verwendeten Verfahrens sichergestellt werden. Sofern Daten im Sinne von Satz 1 an Dritte übermittelt werden, müssen diese ihren Sitz in der Europäischen Union oder einem Schengen-assoziierten Staat haben. Die Übermittlung personenbezogener Daten zur Durchführung der Maßnahme nach Absatz 1 Satz 1 ist nur innerhalb der Europäischen Union, einschließlich der Schengen-assoziierten Staaten, zulässig. Die Weiterverarbeitung von personenbezogenen Daten, die aus in § 12 Absatz 3 genannten Maßnahmen erlangt wurden, ist unzulässig. Eine Übermittlung der in Satz 6 genannten Daten ist unzulässig. Personenbezogene Daten werden nur an solche Personen übermittelt, die Amtsträger oder für den öffentlichen Dienst besonders Verpflichtete sind oder die zur Geheimhaltung verpflichtet worden sind. § 1 Absatz 2, 3 und 4 Nummer 1 des Verpflichtungsgesetzes ist auf die Verpflichtung zur Geheimhaltung entsprechend anzuwenden. Durch organisatorische und technische Maßnahmen hat das Bundeskriminalamt zu gewährleisten, dass die Daten gegen unbefugte Kenntnisnahme geschützt sind.

(4) Die Bundesregierung bestimmt vor der Übermittlung von personenbezogenen Daten an Dritte nach Absatz 3 Satz 1 durch Rechtsverordnung ohne Zustimmung des Bundesrates nach Anhörung der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit das Nähere zu dem technischen Verfahren, den Sicherungsmaßnahmen zur Verhinderung unbefugter Datenzugriffe und nähere Vorgaben zu Art und Umfang der verarbeiteten Daten. In der Rechtsverordnung nach Satz 1 bestimmt sie insbesondere

1. Art der zu verarbeitenden Daten,
2. Definition von unveränderten Daten,
3. Personenkreis, der von der Verarbeitung betroffen ist,
4. Sicherungsmaßnahmen zur Datenaktualität und -qualität,
5. Mindeststandards zur technischen Durchführung der Anonymisierung und Pseudonymisierung von Daten einschließlich einer näheren Bestimmung des unverhältnismäßigen Aufwands im Sinne von Absatz 3 Satz 1 Nummer 2,
6. Protokollierung, einschließlich einer individuellen Kennung der handelnden Personen.“

6. § 33 wird wie folgt geändert:

a) Absatz 1 wird wie folgt geändert:

aa) In Nummer 3 wird das Wort „und“ durch ein Komma ersetzt.

bb) In Nummer 4 wird der Punkt am Ende durch das Wort „und“ ersetzt.

cc) Folgende Nummer 5 wird angefügt:

„5. einen Abgleich nach § 10b Absatz 1 zum Zweck der Identifizierung oder Aufenthaltsermittlung durchführen.“

b) Absatz 4 wird wie folgt geändert:

aa) In Nummer 4 wird der Punkt am Ende durch ein Komma ersetzt.

bb) Folgende Nummer 5 wird angefügt:

„5. einen Abgleich nach § 10b Absatz 1 zum Zweck der Identifizierung oder Aufenthaltsermittlung durchführen.“

7. Nach § 63a wird folgender § 63b eingefügt:

„§ 63b

Nachträglicher biometrischer Abgleich mit allgemein öffentlich zugänglichen Daten aus dem Internet; Verordnungsermächtigung

(1) Das Bundeskriminalamt kann biometrische Daten zu Gesichtern und Stimmen, auf die es zur Erfüllung seiner Aufgaben zugreifen darf, mit allgemein öffentlich zugänglichen personenbezogenen Daten aus dem Internet mittels einer automatisierten Anwendung zur Datenverarbeitung biometrisch abgleichen, sofern dies im Einzelfall erforderlich ist zur Identifizierung oder Ermittlung des Aufenthaltsorts der Zielperson

1. zur Abwehr einer erheblichen Gefahr für Leib, Leben oder Freiheit für eine zu schützende Person oder für eine zu schützende Räumlichkeit nach § 6 oder
2. zum Schutz von Leib, Leben, Freiheit sexueller Selbstbestimmung oder bedeutenden Sachwerten einer zu schützenden Person oder zum Schutz einer zu schützenden Räumlichkeit nach § 6 vor einer gemeingefährlichen Straftat, wenn Tatsachen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, an dem bestimmte Personen beteiligt sein werden, oder
3. zum Schutz von Leib, Leben, Freiheit oder sexueller Selbstbestimmung einer zu schützenden Person oder zum Schutz einer zu schützenden Räumlichkeit nach § 6 vor einer gemeingefährlichen Straftat, wenn das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie in einem übersehbaren Zeitraum eine Straftat gegen eines dieser Rechtsgüter der zu schützenden Person oder gegen eine zu schützende Räumlichkeit begehen wird,

und die Gefahr nach den Nummern 1 bis 3 auch im Einzelfall von erheblicher Bedeutung ist sowie die Abwehr der Gefahr auf andere Weise aussichtlos oder wesentlich erschwert wäre. Ein Abgleich mit Daten nach Satz 1 aus im Internet allgemein öffentlich zugänglichen in Echtzeit erhobenen Daten ist ausgeschlossen.

(2) Die Maßnahme nach Absatz 1 Satz 1 darf gegen die entsprechend § 17 oder § 18 des Bundespolizeigesetzes Verantwortlichen sowie Personen im Sinne von Absatz 1 Satz 2 Nummer 1 oder 2 durchgeführt werden.

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

(4) Maßnahmen nach Absatz 1 Satz 1 dürfen 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 auch durch die Präsidentin oder den Präsidenten des Bundeskriminalamtes oder ihrer oder seiner Vertretung getroffen werden. Sofern die Anordnung der Präsidentin oder des Präsidenten des Bundeskriminalamtes oder ihrer oder seiner Vertretung nicht binnen drei Tagen von dem Gericht bestätigt wird, tritt sie außer Kraft. Die Anordnung ergeht schriftlich. In ihrer Entscheidungsformel sind anzugeben:

1. die Person, zu deren Identifizierung oder Aufenthaltsermittlung die Maßnahme angeordnet wird,

2. die biometrischen Daten aus dem Strafverfahren oder dem Vorgang, die dieser Person zuzuordnen sind und die zum Abgleich herangezogen werden sollen,

3. der Tatvorwurf oder Sachverhalt, auf Grund dessen die Maßnahme angeordnet wird, und

4. die eingesetzte automatisierte Anwendung zur Datenverarbeitung.

(5) In der Begründung der Anordnung sind die Voraussetzungen für die Maßnahme nach Absatz 1 Satz 1 und die wesentlichen Abwägungsgesichtspunkte darzulegen. Insbesondere sind einzelfallbezogen die bestimmten Tatsachen, die den Verdacht begründen, die wesentlichen Erwägungen zur Erforderlichkeit und Verhältnismäßigkeit der Maßnahme, die wesentlichen Einzelheiten zur technischen Funktionsweise der automatisierten Anwendung zur Datenverarbeitung sowie die Subsidiarität zu anderen Maßnahmen anzugeben.

(6) Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch eine Maßnahme nach Absatz 1 Satz 1 allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt werden, ist die Maßnahme unzulässig. Erkenntnisse aus dem Kernbereich privater Lebensgestaltung, die durch eine Maßnahme nach Absatz 1 Satz 1 erlangt wurden, dürfen nicht verwertet werden. Aufzeichnungen über solche Erkenntnisse sind unverzüglich zu löschen. Die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren. Bei Maßnahmen nach Absatz 1 Satz 1 ist, soweit möglich, technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. Erkenntnisse, die durch Maßnahmen nach Absatz 1 Satz 1 erlangt wurden und den Kernbereich privater Lebensgestaltung betreffen, sind unverzüglich zu löschen oder von der Präsidentin oder dem Präsidenten des Bundeskriminalamtes oder ihrer oder seiner Vertretung dem anordnenden Gericht zur Entscheidung über die Verwertbarkeit und Löschung der Daten vorzulegen. Die Entscheidung des Gerichts über die Verwertbarkeit ist für das weitere Verfahren bindend.

(7) Die im Rahmen des Abgleichs nach Absatz 1 Satz 1 erhobenen Daten sind nach Durchführung des Abgleichs unverzüglich zu löschen, sofern sie keinen konkreten Ermittlungsansatz für den Ausgangssachverhalt aufweisen. Die Weiterverarbeitung der beim Abgleich erhobenen Daten ist im Übrigen unzulässig.

(8) Bei jeder Maßnahme nach Absatz 1 Satz 1 ist die Bezeichnung der eingesetzten automatisierten Anwendung zur Datenverarbeitung, der Zeitpunkt ihres Einsatzes sowie die Organisationseinheit einschließlich einer individuellen Kennung der Person, die die Maßnahme durchführt, zu protokollieren. Nach Beendigung einer Maßnahme nach Absatz 1 ist die Stelle zu unterrichten, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz bei öffentlichen Stellen zuständig ist.

(9) Soweit zur Durchführung des Abgleichs nach Absatz 1 Satz 1 Dritte im Wege der Auftragsverarbeitung für das Bundeskriminalamt tätig werden, müssen diese ihren Sitz in der Europäischen Union oder einem Schengen-assoziierten Staat haben. Die Übermittlung personenbezogener Daten zur Durchführung der Maßnahme nach Absatz 1 Satz 1 ist nur innerhalb der Europäischen Union, einschließlich der Schengen-assoziierten Staaten, zulässig. Die Weiterverarbeitung durch Dritte von personenbezogenen Daten, die aus in § 12 Absatz 3 genannten Maßnahmen erlangt wurden, ist ausgeschlossen. Personenbezogene Daten werden nur an solche Personen übermittelt, die Amtsträger oder für den öffentlichen Dienst besonders Verpflichtete sind oder die zur Geheimhaltung verpflichtet worden sind. § 1 Absatz 2, 3 und 4 Nummer 1 des Verpflichtungsgesetzes ist auf die Verpflichtung zur Geheimhaltung entsprechend anzuwenden. Durch organisatorische und technische Maßnahmen ist zu gewährleisten, dass die Daten gegen unbefugte Kenntnisnahme geschützt sind.

(10) Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit führt Kontrollen bezüglich der Datenverarbeitung der Maßnahme nach Absatz 1 Satz 1 mindestens alle zwei Jahre durch.

(11) Die Bundesregierung bestimmt vor dem Einsatz von Maßnahmen nach Absatz 1 Satz 1 durch Rechtsverordnung ohne Zustimmung des Bundesrates nach Anhörung der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit das Nähere zu dem technischen Verfahren, den Sicherungsmaßnahmen zur Verhinderung unbefugter Datenzugriffe und, soweit eine Speicherung der abzugleichenden, öffentlich zugänglichen Lichtbild- Video- und Audiodateien für die Durchführung von Maßnahmen nach Absatz 1 technisch erforderlich ist, nähere Vorgaben zu Art, Umfang und Dauer. In der Rechtsverordnung nach Satz 1 bestimmt sie insbesondere

1. Eingabe- und Zugangsberechtigung,

2. Speicher- und Löschfristen,
3. Art der zu speichernden Daten,
4. Personenkreis, der von der Speicherung betroffen ist,
5. Dauer der Speicherung,
6. Protokollierung.“

Artikel 2

Änderung des Bundespolizeigesetzes

Das Bundespolizeigesetz vom 19. Oktober 1994 (BGBl. I S. 2978, 2979), das zuletzt durch Artikel 5 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nr. 149) geändert worden ist, wird wie folgt geändert:

1. In der Inhaltsübersicht werden nach der Angabe zu § 34 die folgenden Angaben eingefügt:

   „§ 34a Automatisierte Datenanalyse; Verordnungsermächtigung

   § 34b Nachträglicher biometrischer Abgleich mit allgemein öffentlich zugänglichen Daten aus dem Internet; Verordnungsermächtigung“.

2. Nach § 22 Absatz 1a wird folgender Absatz 1b eingefügt:

   „(1b) Die Bundespolizei kann zur Durchsetzung von Waffenverbotszonen nach § 42b Absatz 2 des Waffengesetzes sowie zur Durchsetzung von Allgemeinverfügungen der Bundespolizei auf dem Gebiet der Bahnanlagen der Eisenbahnen des Bundes, welche das Mitführen von konkret bezeichneten gefährlichen Gegenständen und Waffen untersagt, in den jeweiligen räumlichen Geltungsbereichen Personen kurzzeitig anhalten, befragen und verlangen, dass mitgeführte Ausweispapiere zur Prüfung ausgehändigt werden, sowie mitgeführte Sachen in Augenschein nehmen und durchsuchen. Die Auswahl der nach Satz 1 durch die Bundespolizei kontrollierten Person anhand eines Merkmals im Sinne des Artikels 3 Absatz 3 des Grundgesetzes ohne sachlichen, durch den Zweck der Maßnahme gerechtfertigten Grund ist unzulässig.“

3. Nach § 34 werden die folgenden §§ 34a und 34b eingefügt:

„§ 34a

Automatisierte Datenanalyse; Verordnungsermächtigung

(1) Die Bundespolizei kann zur Erfüllung ihrer Aufgaben nach den §§ 1 bis 8 personenbezogene Daten, die sie zur Erfüllung der ihr obliegenden Aufgaben weiterverarbeitet oder für die sie eine Berechtigung zum Abruf hat, mittels einer automatisierten Anwendung zur Datenverarbeitung zusammenführen und darüber hinaus zum Zwecke der Analyse weiterverarbeiten, sofern

1. 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, erforderlich ist,
2. bestimmte Tatsachen die Annahme rechtfertigen, dass eine Person innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Straftat von auch im Einzelfall erheblicher Bedeutung im Zusammenhang mit lebensgefährdenden Schleusungen oder eine Straftat von auch im Einzelfall erheblicher Bedeutung, die gegen die Sicherheit der Anlagen oder des Betriebes des Luft-, See- oder Bahnverkehrs, insbesondere Straftaten von auch im Einzelfall erheblicher Bedeutung nach den §§ 315, 315b, 316b und 316c des Strafgesetzbuches, gerichtet ist und eine nicht unerhebliche Gefährdung eines der in Nummer 1 genannten Rechtsgüter erwarten lässt, begehen wird, und dies zur Verhütung der Straftat erforderlich ist, oder

3. das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums eine Straftat von auch im Einzelfall erheblicher Bedeutung im Zusammenhang mit lebensgefährdenden Schleusungen oder eine Straftat von auch im Einzelfall erheblicher Bedeutung, die gegen die Sicherheit der Anlagen oder des Betriebes des Luft-, See- oder Bahnverkehrs gerichtet ist, insbesondere Straftaten von auch im Einzelfall erheblicher Bedeutung nach den §§ 315, 315b, 316b und 316c des Strafgesetzbuches, und eine nicht unerhebliche Gefährdung eines der in Nummer 1 genannten Rechtsgüter erwarten lässt, begehen wird, und dies zur Verhütung der Straftat erforderlich ist.

(2) Im Rahmen der Weiterverarbeitung nach den Absatz 1 können insbesondere datei- und informationssystemübergreifend Beziehungen oder Zusammenhänge zwischen Personen, Personengruppierungen, Institutionen, Organisationen, Objekten und Sachen hergestellt, unbedeutende Informationen und Erkenntnisse ausgeschlossen, Suchkriterien gewichtet, die eingehenden Erkenntnisse zu bekannten Sachverhalten zugeordnet sowie gespeicherte Daten statistisch ausgewertet werden.

(3) Beim Einsatz selbstlernender Systeme gilt § 22 Absatz 3 Satz 2 und 3 des Bundeskriminalamtgesetzes entsprechend.

(4) Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit führt Kontrollen bezüglich der Datenverarbeitung der Maßnahme nach Absatz 1 mindestens alle zwei Jahre durch.

(5) Die Bundesregierung bestimmt vor dem Einsatz von Maßnahmen nach Absatz 1 durch Rechtsverordnung ohne Zustimmung des Bundesrates nach Anhörung der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit das Nähere zu dem technischen Verfahren, den Sicherungsmaßnahmen zur Verhinderung unbefugter Datenzugriffe und nähere Vorgaben zu Art und Umfang der verarbeiteten Daten. In der Rechtsverordnung nach Satz 1 bestimmt sie insbesondere

1. Eingabe- und Zugangsberechtigung,
2. Art der zu verarbeitenden Daten,
3. Personenkreis, der von der Verarbeitung betroffen ist,
4. besondere Regelungen über die Verarbeitung von Daten, die durch besonders eingriffsintensive Maßnahmen erhoben wurden,
5. Protokollierung, einschließlich einer individuellen Kennung der handelnden Personen.

§ 34b

Nachträglicher biometrischer Abgleich mit allgemein öffentlich zugänglichen Daten aus dem Internet; Verordnungsermächtigung

(1) Die Bundespolizei kann biometrische Daten zu Gesichtern und Stimmen, die sie zur Erfüllung ihrer Aufgaben nach den §§ 1 bis 8 weiterverarbeitet oder für die sie eine Berechtigung zum Abruf hat, mit allgemein öffentlich zugänglichen personenbezogenen Daten aus dem Internet mittels einer automatisierten Anwendung zur Datenverarbeitung biometrisch abgleichen, sofern

1. dies im Rahmen der 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, zur Identifizierung oder Ermittlung des Aufenthaltsorts der Zielperson erforderlich ist und
2. die Abwehr der Gefahr auf andere Weise aussichtslos ist oder wesentlich erschwert wäre.

Die Maßnahme nach Satz 1 ist auch zulässig, sofern im Rahmen der Aufgaben nach den §§ 1 bis 8

1. bestimmte Tatsachen die Annahme rechtfertigen, dass eine Person innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Straftat von auch im Einzelfall erheblicher Bedeutung im Zusammenhang mit lebensgefährdenden Schleusungen oder eine Straftat von auch im Einzelfall erheblicher Bedeutung, die gegen die Sicherheit der Anlagen oder des Betriebes des

Luft-, See- oder Bahnverkehrs, insbesondere Straftaten von auch im Einzelfall erheblicher Bedeutung nach den §§ 315, 315b, 316b und 316c des Strafgesetzbuches, gerichtet ist und eine nicht unerhebliche Gefährdung eines der in Satz 1 Nummer 1 genannten Rechtsgüter erwarten lässt, begehen wird, oder

2. das individuelle Verhalten einer Person die konkrete Wahrscheinlichkeit begründet, dass sie innerhalb eines übersehbaren Zeitraums eine Straftat von auch im Einzelfall erheblicher Bedeutung im Zusammenhang mit lebensgefährdenden Schleusungen oder eine Straftat von auch im Einzelfall erheblicher Bedeutung, die gegen die Sicherheit der Anlagen oder des Betriebes des Luft-, See- oder Bahnverkehrs gerichtet ist, insbesondere Straftaten von auch im Einzelfall erheblicher Bedeutung nach den §§ 315, 315b, 316b und 316c des Strafgesetzbuches, und eine nicht unerhebliche Gefährdung eines der in Satz 1 Nummer 1 genannten Rechtsgüter erwarten lässt, begehen wird

und die Verhütung der Straftat auf andere Weise aussichtslos oder wesentlich erschwert wäre. Ein Abgleich mit Daten nach Satz 1 aus im Internet allgemein öffentlich zugänglichen in Echtzeit erhobenen Daten ist ausgeschlossen.

(2) Die Maßnahme nach Absatz 1 Satz 1 darf gegen die nach § 17 oder § 18 Verantwortlichen sowie Personen im Sinne von Absatz 1 Satz 2 Nummer 1 oder 2 durchgeführt werden.

(3) Maßnahmen nach Absatz 1 Satz 1 dürfen nur auf Antrag der Präsidentin oder des Präsidenten des Bundespolizeipräsidiums oder ihrer oder seiner Vertretung durch das Gericht angeordnet werden. Für das Verfahren gelten die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit mit Ausnahme des § 23 Absatz 2 und des § 37 Absatz 2 entsprechend. Die Anordnung wird mit Erlass wirksam. Bei Gefahr im Verzug kann die Anordnung auch durch die Präsidentin oder den Präsidenten des Bundespolizeipräsidiums oder ihre oder seine Vertretung getroffen werden. Sofern die Anordnung der Präsidentin oder des Präsidenten des Bundespolizeipräsidiums oder ihrer oder seiner Vertretung nicht binnen drei Tagen von dem Gericht bestätigt wird, tritt sie außer Kraft. Die Anordnung ergeht schriftlich. In ihrer Entscheidungsformel sind anzugeben:

1. die Person, zu deren Identifizierung oder Aufenthaltsermittlung die Maßnahme angeordnet wird,
2. die biometrischen Daten aus dem Vorgang, die dieser Person zuzuordnen sind und die zum Abgleich herangezogen werden sollen,
3. der Sachverhalt, auf Grund dessen die Maßnahme angeordnet wird, und
4. die eingesetzte automatisierte Anwendung zur Datenverarbeitung.

(4) In der Begründung der Anordnung sind die Voraussetzungen für die Maßnahme nach Absatz 1 Satz 1 und die wesentlichen Abwägungsgesichtspunkte darzulegen. Insbesondere sind einzelfallbezogen die bestimmten Tatsachen, die den Verdacht begründen, die wesentlichen Erwägungen zur Erforderlichkeit und Verhältnismäßigkeit der Maßnahme, die wesentlichen Einzelheiten zur technischen Funktionsweise der automatisierten Anwendung zur Datenverarbeitung sowie die Subsidiarität zu anderen Maßnahmen anzugeben.

(5) Liegen tatsächliche Anhaltspunkte für die Annahme vor, dass durch eine Maßnahme nach Absatz 1 Satz 1 allein Erkenntnisse aus dem Kernbereich privater Lebensgestaltung erlangt werden, ist die Maßnahme unzulässig. Erkenntnisse aus dem Kernbereich privater Lebensgestaltung, die durch eine Maßnahme nach Absatz 1 Satz 1 erlangt wurden, dürfen nicht verwertet werden. Aufzeichnungen über solche Erkenntnisse sind unverzüglich zu löschen. Die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren. Bei Maßnahmen nach Absatz 1 Satz 1 ist, soweit möglich, technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. Erkenntnisse, die durch Maßnahmen nach Absatz 1 Satz 1 erlangt wurden und den Kernbereich privater Lebensgestaltung betreffen, sind unverzüglich zu löschen oder von der Präsidentin oder dem Präsidenten des Bundespolizeipräsidiums oder ihrer oder seiner Vertretung dem anordnenden Gericht zur Entscheidung über die Verwertbarkeit und Löschung der Daten vorzulegen. Die Entscheidung des Gerichts über die Verwertbarkeit ist für das weitere Verfahren bindend.

(6) Die im Rahmen des Abgleichs nach Absatz 1 Satz 1 erhobenen Daten sind nach Durchführung des Abgleichs unverzüglich zu löschen, sofern sie keinen konkreten Ermittlungsansatz für den Ausgangssachverhalt aufweisen. Die Weiterverarbeitung der beim Abgleich erhobenen Daten ist im Übrigen unzulässig.

(7) Bei jeder Maßnahme nach Absatz 1 Satz 1 ist die Bezeichnung der eingesetzten automatisierten Anwendung zur Datenverarbeitung, der Zeitpunkt ihres Einsatzes sowie die Organisationseinheit einschließlich einer individuellen Kennung der Person, die die Maßnahme durchführt, zu protokollieren. Nach Beendigung einer Maßnahme nach Absatz 1 ist die Stelle zu unterrichten, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz bei öffentlichen Stellen zuständig ist.

(8) Soweit zur Durchführung des Abgleichs nach Absatz 1 Satz 1 Dritte im Wege der Auftragsverarbeitung für die Bundespolizei tätig werden, müssen diese ihren Sitz in der Europäischen Union oder einem Schengen-assoziierten Staat haben. Die Übermittlung personenbezogener Daten zur Durchführung der Maßnahme nach Absatz 1 Satz 1 ist nur innerhalb der Europäischen Union, einschließlich der Schengen-assoziierten Staaten, zulässig. Personenbezogene Daten werden nur an solche Personen übermittelt, die Amtsträger oder für den öffentlichen Dienst besonders Verpflichtete sind oder die zur Geheimhaltung verpflichtet worden sind. § 1 Absatz 2, 3 und 4 Nummer 1 des Verpflichtungsgesetzes ist auf die Verpflichtung zur Geheimhaltung entsprechend anzuwenden. Durch organisatorische und technische Maßnahmen ist zu gewährleisten, dass die Daten gegen unbefugte Kenntnisnahme geschützt sind.

(9) Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit führt Kontrollen bezüglich der Datenverarbeitung der Maßnahme nach Absatz 1 Satz 1 mindestens alle zwei Jahre durch.

(10) Die Bundesregierung bestimmt vor dem Einsatz von Maßnahmen nach Absatz 1 Satz 1 durch Rechtsverordnung ohne Zustimmung des Bundesrates nach Anhörung der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit das Nähere zu dem technischen Verfahren, den Sicherungsmaßnahmen zur Verhinderung unbefugter Datenzugriffe und, soweit eine Speicherung der abzugleichenden, öffentlich zugänglichen Lichtbild- Video- und Audiodateien für die Durchführung von Maßnahmen nach Absatz 1 technisch erforderlich ist, nähere Vorgaben zu Art, Umfang und Dauer. In der Rechtsverordnung nach Satz 1 bestimmt sie insbesondere

1. Eingabe- und Zugangsberechtigung,
2. Speicher- und Löschfristen,
3. Art der zu speichernden Daten,
4. Personenkreis, der von der Speicherung betroffen ist,
5. Dauer der Speicherung,
6. Protokollierung.“

4. § 43 Absatz 1 wird wie folgt geändert:
   a) In Nummer 3 wird das Wort „oder“ am Ende durch ein Komma ersetzt.
   b) In Nummer 4 wird der Punkt am Ende durch das Wort „oder“ ersetzt.
   c) Folgende Nummer 5 wird angefügt:
      „5. Maßnahmen nach § 22 Absatz 1b durchgeführt werden.“

Artikel 3

Änderung der Strafprozessordnung

Die Strafprozessordnung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch Artikel 2 Absatz 1 des Gesetzes vom 7. November 2024 (BGBl. 2024 I Nr. 351) geändert worden ist, wird wie folgt geändert:

1. In der Inhaltsübersicht wird nach der Angabe zu § 98c folgende Angabe eingefügt:
   „§ 98d Nachträglicher Abgleich biometrischer Daten mit im Internet allgemein öffentlich zugänglichen Daten mittels einer automatisierten Anwendung zur Datenverarbeitung; Verordnungsermächtigung“.

2. Nach § 98c wird folgender § 98d eingefügt:

„§ 98d

Nachträglicher Abgleich biometrischer Daten mit im Internet allgemein öffentlich zugänglichen Daten mittels einer automatisierten Anwendung zur Datenverarbeitung; Verordnungsermächtigung

(1) Zur Identitätsfeststellung oder Ermittlung des Aufenthaltsorts eines Beschuldigten oder eines Verletzten durch Erkennung des Gesichts und der Stimme dürfen deren biometrische Daten aus einem Strafverfahren mit biometrischen Daten aus im Internet allgemein öffentlich zugänglichen Lichtbild-, Audio- und Videodateien nachträglich mittels einer automatisierten Anwendung zur Datenverarbeitung abgeglichen werden, wenn

1. bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine in § 100b Absatz 2 bezeichnete besonders schwere Straftat begangen, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht oder durch eine Straftat vorbereitet hat,
2. die Tat auch im Einzelfall besonders schwer wiegt und
3. die Identitätsfeststellung oder die Ermittlung des Aufenthaltsortes auf andere Weise wesentlich erschwert oder aussichtslos wäre.

Ein Abgleich mit Daten nach Satz 1 aus im Internet öffentlich zugänglichen in Echtzeit erhobenen Daten ist ausgeschlossen. Die Identitätsfeststellung oder Ermittlung des Aufenthaltsorts des Verletzten hat zu unterbleiben, wenn überwiegende schutzwürdige Interessen des Verletzten entgegenstehen.

(2) Maßnahmen nach Absatz 1 dürfen nur auf Antrag der Staatsanwaltschaft durch das Gericht angeordnet werden. Bei Gefahr im Verzug kann die Anordnung auch durch die Staatsanwaltschaft getroffen werden. Soweit die Anordnung der Staatsanwaltschaft nicht binnen drei Tagen von dem Gericht bestätigt wird, tritt sie außer Kraft. Die Anordnung ergeht schriftlich. In ihrer Entscheidungsformel sind anzugeben:

1. die Person, zu deren Identifizierung oder Aufenthaltsermittlung die Maßnahme angeordnet wird,
2. die biometrischen Daten aus dem Strafverfahren, die dieser Person zuzuordnen sind und die zum Abgleich herangezogen werden sollen,
3. der Tatvorwurf, auf Grund dessen die Maßnahme angeordnet wird, und
4. die zur Datenverarbeitung eingesetzte automatisierte Anwendung.

(3) In der Begründung der Anordnung sind die Voraussetzungen für die Maßnahme nach Absatz 1 und die wesentlichen Abwägungsgesichtspunkte darzulegen. Insbesondere sind einzelfallbezogen die bestimmten Tatsachen, die den Verdacht begründen, die wesentlichen Erwägungen zur Erforderlichkeit und Verhältnismäßigkeit der Maßnahme, die wesentlichen Einzelheiten zur technischen Funktionsweise der automatisierten Anwendung zur Datenverarbeitung sowie die Subsidiarität zu anderen Maßnahmen anzugeben.

(4) § 100d Absatz 1 bis 3 gilt entsprechend.

(5) Die im Rahmen des Abgleichs nach Absatz 1 Satz 1 erhobenen Daten sind nach Durchführung des Abgleichs unverzüglich zu löschen, soweit sie keinen konkreten Ermittlungsansatz aufweisen. Dies gilt auch für sonstige erhobene Daten, soweit schutzwürdige Interessen des Betroffenen im Einzelfall gegenüber dem Strafverfolgungsinteresse überwiegen. Im Fall des Absatzes 2 Satz 3 sind alle bereits erhobenen Daten unverzüglich zu löschen. Die Löschung ist aktenkundig zu machen. Die Weiterverarbeitung der beim Abgleich erhobenen Daten ist im Übrigen unzulässig.

(6) Bei jeder Maßnahme sind die Bezeichnung der eingesetzten automatisierten Anwendung zur Datenverarbeitung, der Zeitpunkt ihres Einsatzes und die Organisationseinheit, die die Maßnahme durchführt, einschließlich einer individuellen Kennung der Person, die die Maßnahme durchführt, zu protokollieren. Nach Beendigung einer Maßnahme nach Absatz 1 ist die Stelle zu unterrichten, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz bei öffentlichen Stellen zuständig ist.

(7) Dritte dürfen im Rahmen einer Auftragsverarbeitung nur tätig werden, wenn sichergestellt ist, dass die Verarbeitung personenbezogener Daten im Rahmen des Abgleichs nur durch Amtsträger oder für den öffentlichen Dienst besonders Verpflichtete oder zur Geheimhaltung verpflichtete Mitarbeiterinnen oder Mitarbeiter erfolgt. § 1 Absatz 2, 3 und 4 des Verpflichtungsgesetzes ist auf die Verpflichtung zur Geheimhaltung entsprechend anzuwenden. Durch organisatorische und technische Maßnahmen ist zu gewährleisten, dass die Daten gegen unbefugte Kenntnisnahme geschützt sind. Sofern zur Durchführung des Abgleichs nach Absatz 1 Satz 1 Dritte im Wege der Auftragsverarbeitung tätig werden, müssen diese ihren Sitz in der Europäischen Union oder einem Schengen-assoziierten Staat haben. Die Übermittlung personenbezogener Daten zur Durchführung der Maßnahme nach Absatz 1 Satz 1 ist nur innerhalb der Europäischen Union, einschließlich der Schengen-assoziierten Staaten, zulässig.

(8) Die Bundesregierung bestimmt vor dem Einsatz von Maßnahmen nach Absatz 1 durch Rechtsverordnung mit Zustimmung des Bundesrates nach Anhörung der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit das Nähere zu dem technischen Verfahren, den Sicherungsmaßnahmen zur Verhinderung unbefugter Datenzugriffe und, sofern eine Speicherung der abzugleichenden, allgemein öffentlich zugänglichen Lichtbild- Video- und Audiodateien für die Durchführung von Maßnahmen nach Absatz 1 technisch erforderlich ist, nähere Vorgaben zu Art, Umfang und Dauer. In der Rechtsverordnung nach Satz 1 bestimmt sie insbesondere

1. nähere Vorgaben für die Eingabe- und Zugangsberechtigung,
2. die Speicher- und Löschfristen,
3. die Art und den Umfang der zu speichernden Daten und
4. die Dauer der Speicherung.

(9) Die Stelle, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz bei öffentlichen Stellen zuständig ist, führt mindestens alle zwei Jahre Kontrollen über die die Maßnahme nach Absatz 1 betreffende Datenverarbeitung durch.“

3. § 101 wird wie folgt gefasst:

a) In Absatz 1 wird nach der Angabe „98a,“ die Angabe „98d,“ eingefügt.

b) Nach Absatz 4 Satz 1 Nummer 1 wird folgende Nummer 1a eingefügt:

„1a. des § 98d die Person, zu deren Identifizierung oder Aufenthaltsermittlung die Maßnahme angeordnet wurde.“

Artikel 4

Evaluierung

Das Bundesministerium des Innern und für Heimat und das Bundesministerium der Justiz beauftragen gemeinsam eine fachunabhängige wissenschaftliche Einrichtung, die Anwendung von §§ 10b, 16a und 63b des Bundeskriminalamtgesetzes, §§ 34a und 34b des Bundespolizeigesetzes und § 98d der Strafprozessordnung zu evaluieren. Der Evaluierungszeitraum beginnt am … [einsetzen: 1. Januar des auf das Datum des Inkrafttretens dieses Gesetzes folgenden Jahres] und beträgt drei Jahre.

Artikel 5

Inkrafttreten

Dieses Gesetz tritt am Tag nach der Verkündung in Kraft.

Berlin, den 28. Januar 2025

Dr. Rolf Mützenich und Fraktion
Katharina Dröge, Britta Haßelmann und Fraktion

Begründung

A. Allgemeiner Teil

I. Zielsetzung und Notwendigkeit der Regelungen

Dieser Gesetzentwurf dient insbesondere der Stärkung digitaler Befugnisse der Sicherheitsbehörden.

Die Messerattacke von Aschaffenburg am 22. Januar 2025, der Anschlag auf den Weihnachtsmarkt in Magdeburg am 22. Dezember 2024 und der islamistische Anschlag am 23. August 2024 auf einem Volksfest in Solingen haben deutlich gemacht, dass sich die Sicherheits- und Bedrohungslage in Deutschland erheblich verschärft hat. Auch vor diesem Hintergrund sollen mit dem vorgelegten Gesetzentwurf die Befugnisse der Sicherheitsbehörden bei Gefahrenabwehr und Strafverfolgung gestärkt werden.

Erfolgreiche Polizeiarbeit erfordert moderne und sachgerechte polizeiliche Befugnisse. Dies betrifft angesichts der aktuellen Herausforderungen zunehmend die digitale Welt. Bundeskriminalamt und Bundespolizei benötigen vor diesem Hintergrund Zugriff auf die erforderlichen Daten und müssen über die notwendigen Instrumente verfügen, Daten aufzubereiten und auszuwerten. Der Gesetzentwurf verfolgt das Ziel, das Bundeskriminalamt bei der Erfüllung der Aufgaben als Zentralstelle der deutschen Polizeibehörden und dem Schutz von Verfassungsorganen sowie die Bundespolizei – insbesondere beim Grenzschutz – mit zeitgemäßen Befugnissen auszustatten.

Zudem soll für alle Strafverfolgungsbehörden eine ausdrückliche Ermächtigungsgrundlage geschaffen werden, die den Abgleich von öffentlich zugänglichen Daten aus dem Internet mit Lichtbildern und Stimmen von Tatverdächtigen und anderen gesuchten Personen auf eine rechtssichere Grundlage stellt.

Waffenverbotszonen und Allgemeinverfügungen, die das Mitführen von Waffen und gefährlichen Gegenständen verbieten, können nur eine Wirkung entfalten, wenn sie durchgesetzt werden. Hierzu bedarf es neuer Befugnisse für die Bundespolizei zur Kontrolle von Personen auf dem Gebiet der Eisenbahnen des Bundes, wenn dort das Mitführen von Waffen oder gefährlichen Gegenständen untersagt ist.

II. Wesentlicher Inhalt des Entwurfs

Für den biometrischen Internetabgleich, die automatisierte Datenanalyse, BKA-Anfragen bei Banken sowie Waffenverbotszonen sollen neue Befugnisse geschaffen werden:

Die Befugnis zum biometrischen Abgleich von öffentlich zugänglichen Daten aus dem Internet dient dem Zweck, dass die Strafverfolgungsbehörden zu Strafverfolgungszwecken sowie darüber hinaus das Bundeskriminalamt und die Bundespolizei für weitere (polizeiliche Aufgaben) biometrische Daten zu Gesichtern und Stimmen mittels automatisierter technischer Verfahren mit Internetdaten (z. B. soziale Medien), abgleichen können. Ziel ist es insbesondere, Tatverdächtige zu identifizieren und zu lokalisieren.

Digitalisierung führt dazu, dass Datenmengen grundsätzlich ansteigen und weiter ansteigen werden, sowie zunehmend große Datenmengen aufbereitet und ausgewertet werden müssen. Hierfür sollen Befugnisse zur automatisierten Datenanalyse für Bundeskriminalamt und Bundespolizei geschaffen werden. Diese Befugnisse können dazu dienen, bei großen Datenmengen, Verbindungen/Beziehungen zwischen Informationen herzustellen. Die Polizeibehörden werden auf diese Weise in die Lage versetzt, bereits im polizeilichen Informationssystem oder im polizeilichen Informationsverbund vorhandene Informationen besser, schneller und effizienter auszuwerten. Damit entsprechende IT- und KI-Systeme auch ordnungsgemäß getestet und trainiert werden, bedarf es zur Rechtssicherheit einer entsprechenden Rechtsgrundlage.

Bei Ermittlungen des Bundeskriminalamts kann es erforderlich sein, polizeiliche Anfragen an geldwäscherechtlich Verpflichtete wie z. B. Banken zu stellen. Damit Banken in der Folge nicht das Konto der betroffenen Person kündigen, ist eine Vorschrift im Gesetzentwurf enthalten, die den Banken bei der Kontofortführung

Rechtssicherheit gibt. Damit soll eine verfrühte Unterrichtung der Betroffenen – und damit mögliche Beeinträchtigung der Polizeiarbeit – vermieden werden.

Gegenstand ist ebenfalls eine Befugnis, die anlassbezogen im Falle der Anordnung von Waffenverbotszonen oder im Geltungsbereich von Allgemeinverfügungen der Bundespolizei die stichprobenartige Befragung, Identitätskontrolle sowie Durchsuchung von Personen erlaubt, die die Waffenverbotszone betreten möchten oder sich darin befinden.

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 aus Artikel 73 Absatz 1 Nummer 10 Buchstabe a des Grundgesetzes, für die Änderung der Strafprozessordnung (StPO) aus Artikel 74 Absatz 1 Nummer 1 des Grundgesetzes, für die Änderung des Bundespolizeigesetzes aus Artikel 73 Absatz 1 Nummer 5 (Grenzschutz), 6 (Luftverkehr) und 6a (Eisenbahnen) des Grundgesetzes sowie für die datenschutzrechtlichen Regelungen als Annex zu den jeweiligen Sachkompetenzen. Soweit der Schutz von Bundesorganen, Mitgliedern der Verfassungsorgane und der Leitung des Bundeskriminalamts im Bundeskriminalamt und im Bundespolizeigesetz betroffen ist, folgt die Gesetzgebungskompetenz aus der Natur der Sache.

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. Der Gesetzentwurf dient der Umsetzung der Richtlinie (EU) 2023/977.

VII. Gesetzesfolgen

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

Die neue Befugnis ermöglicht der Bundespolizei die stichprobenartige Kontrolle von Personen bis hin zu Durchsuchung von Personen in bestehenden Waffenverbotszonen oder im Geltungsbereich von entsprechenden Allgemeinverfügungen.

Im Bereich der Eisenbahnen des Bundes sind Schwerpunktmaßnahmen nur effektiv, wenn eine bestimmte Zahl von Personen stichprobenartig kontrolliert wird. Im Ein- und Ausgangsbereich von Bahnhöfen kann dies Auswirkungen auf den Zu- und Abfluss von Personen haben.

1. Rechts- und Verwaltungsvereinfachung

Die Regelungen des Gesetzentwurfs werden nicht zu einer Rechts- oder Verwaltungsvereinfachung führen.

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. Zudem fördert die Sicherheit von Bahnhofsbereichen die Punkte Energiewende und Klimaschutz sowie Verkehrswende, da das Sicherheitsempfinden in den Anlagen der Eisenbahnen des Bundes wesentlich dazu beiträgt, dass das Verkehrsmittel Bahn genutzt wird.

3. Haushaltsausgaben ohne Erfüllungsaufwand

Es entstehen keine Haushaltsausgaben ohne Erfüllungsaufwand.

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

Für Softwarebeschaffung bzw. -entwicklung und -betrieb entstehen Aufwände, ferner weitere sächliche und personelle Aufwände, die in den Folgejahren aufwachsend sein werden, sich derzeit aber insgesamt noch nicht beziffern lassen. Die Aufwände entstehen beim Bundeskriminalamt, bei der Bundespolizei sowie bei den Strafverfolgungsbehörden.

5. Weitere Kosten

Weitere Kosten sind nicht zu erwarten.

6. Weitere Gesetzesfolgen

Das Vorhaben wirkt sich positiv auf den Faktor „Daseinsvorsorge“ aus, da die Sicherheit in Bereichen des öffentlichen Personenverkehrs wesentliche Voraussetzung für eine gleichberechtigte Teilhabe am wirtschaftlichen und sozialen Leben ist. Auswirkungen auf demografierelevante Belange sind nicht zu erwarten.

VIII. Befristung; Evaluierung

Eine Evaluierung ist nach Artikel 4 vorgesehen.

B. Besonderer Teil

Zu Artikel 1 (Änderung des Bundeskriminalamtgesetzes)

Zu Nummer 1

Zu Buchstabe a

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

Zu Buchstabe b

Es handelt sich um eine redaktionelle Folgeänderung zur Einführung von § 16a.

Zu Buchstabe c

Es handelt sich um eine redaktionelle Folgeänderung zur Veränderung der Überschrift von § 22.

Zu Buchstabe d

Es handelt sich um eine redaktionelle Folgeänderung zur Einführung von § 63b.

Zu Nummer 2

Erhebt das Bundeskriminalamt – beispielsweise im Bereich der Terrorismusfinanzierung – Daten zu Personen bspw. bei Kreditinstituten mittels Auskunftsersuchen kann im Einzelfall das Risiko bestehen, dass diese die Geschäftsbeziehungen zu den betroffenen Personen kündigen. Eine Kontokündigung bei den Betroffenen im Anfangsstadium eines Vorgangs kann allerdings das Risiko bergen, den Erfolg der Maßnahme zu vereiteln, weil Betroffene (auch ohne expliziten Hinweis) auf polizeiliche Maßnahmen aufmerksam werden und ihr Verhalten entsprechend anpassen. Die Vorschrift schafft Rechtssicherheit für die Verpflichteten. Hierdurch wird klargestellt, dass aus einer Fortsetzung der Geschäftsbeziehung trotz des Eingangs des Auskunftsersuchens keine zivil-, straf- oder öffentlich-rechtlichen Nachteile entstehen, weil die Fortsetzung der Geschäftsbeziehung dann einer gesetzlich normierten öffentlich-rechtlichen Verpflichtung entspricht. Eine solche Regelung wird den Betroffenen schützen, der nicht bereits auf Grund nur von tatsächlichen Anhaltspunkten in seiner wirtschaftlichen Bewegungsfreiheit beschränkt werden soll, ebenso wie die verpflichteten Unternehmen u. a. der Finanzbranche, die keine Verantwortlichkeit oder Haftung bei einer Fortsetzung der Geschäftsbeziehung befürchten müssten (vgl. Bundestagsdrucksache 17/6925, S. 15).

Zu Nummer 3

Ziel des Abgleichs biometrischer Daten von Gesichtern und Stimmen mit öffentlich zugänglichen Daten aus dem Internet ist die Identifizierung und Lokalisierung insbesondere von Störern und Tatverdächtigen. Eine entsprechende Befugnis ist neben der hier betroffenen Zentralstellenregelung zum Schutz von Mitgliedern der Verfassungsorgane und der Leitung des Bundeskriminalamts (§ 63b) vorgesehen.

Das Bundeskriminalamt hat nach § 2 Absatz 2 Nummer 1 als Zentralstelle die Aufgabe, alle zur Verhütung und Verfolgung von Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung nach § 2 Absatz 1 erforderlichen Informationen zu sammeln und auszuwerten. Im Rahmen dieser Aufgabe unterstützt das Bundeskriminalamt unter anderem in den Bereichen politisch motivierter Kriminalität und Staatsschutz die Ermittlungsarbeit der Polizeibehörden des Bundes und der Länder.

Soweit der Anwendungsbereich der Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz) eröffnet ist, gelten die jeweiligen Vorgaben unmittelbar und sind bei der Entwicklung und Nutzung von KI-Systemen zu beachten. Zwingend sicherzustellen ist insbesondere, dass die Rechtskonformität der verwendeten KI-Systeme entsprechend der Verordnung zertifiziert ist. Dies ist in geeigneter Form in der Rechtsverordnung zu konkretisieren. Zur Erprobung von KI-Systemen sollte das Instrument der KI-Reallabore Anwendung finden.

Zu Absatz 1

Unter einem biometrischen Abgleich im Sinne der Vorschrift ist die technisch gestützte Überprüfung der Übereinstimmung von biometrischen Signaturen mit dem Ergebnis einer Übereinstimmungsbewertung zu verstehen. Unter allgemein öffentlich zugängliche Daten fallen solche Daten, die von jedermann verwendet werden können, beispielsweise aus sozialen Medien, soweit sich diese nicht an einen spezifisch abgegrenzten Personenkreis richten (BT-Drs. 20/12806, S. 18). Konkretisierend fallen darunter Daten, wenn sie jede Person ohne oder nach vorheriger Registrierung, Genehmigung oder Entgeltzahlung nutzen kann. Nicht umfasst sind Daten, die einer spezifischen Schwelle unterzogen sind, beispielsweise der Einstellung von Daten in sozialen Medien für einen begrenzten Kreis, dessen Zugang einer Kontrolle unterzogen wird. Privatkommunikation über Messenger-Dienste von sozialen Medien können nicht von der Maßnahme erfasst werden.

Die Befugnis setzt entsprechend § 9 Absatz 1 voraus, dass die Maßnahme nur zur Ergänzung vorhandener Sachverhalt erfolgen kann. Voraussetzungen für ein Tätigwerden des Bundeskriminalamts ist, dass bereits Ermittlungsunterlagen vorliegen (vgl. Bundestagsdrucksache 13/1550, S. 24). Entsprechend der in diesem Entwurf enthaltenen Regelung in §98d der Strafprozessordnung gilt die Schwelle des § 100b der Strafprozessordnung. Die Vorschrift setzt einen Tatverdacht bzw. zur Straftatenverhütung eine zumindest konkretisierte Gefahrenlage voraus.

Öffentlich zugängliche Daten können auch im Rahmen der allgemeinen Ermittlungsbefugnisse erhoben werden. Spezialgesetzlicher Regelungsbedarf besteht jedoch, da Absatz 1 den biometrischen Abgleich öffentlich zugänglicher Daten mittels automatisierter Verarbeitung regelt. Nur mittels einer technischen Anwendung können Lichtbilder und Videos in einer Form zusammengeführt und analysiert werden, die einen Abgleich ermöglicht. Ohne eine solche technische Verarbeitung könnten die erhobenen Daten nicht verwendet werden, da sich öffentlich zugängliche Daten in Format und Struktur von den im Informationssystem oder -verbund gespeicherten Daten unterscheiden.

Mit Absatz 1 Satz 2 wird klargestellt, dass ein Abgleich mit biometrischen Daten aus im Internet öffentlich zugänglichen Echtzeit-Lichtbild- und Echtzeit-Videodateien ausgeschlossen wird, damit hierüber keine Echtzeitüberwachung bestimmter Bereiche stattfinden kann. Erfasst hiervon sind insbesondere Live-Streams, zum Beispiel von Veranstaltungen, in denen auch das Publikum erfasst wird, oder das Live-Video einer Webcam eines öffentlich zugänglichen Ortes. Ausdrücklich erfasst sind auch Echtzeit-Lichtbild-Dateien, also beispielsweise die Bilder von Webcams, die in zeitlich kurzer Abfolge einzelne Lichtbilder ins Internet hochladen.

Zu Absatz 2

Adressaten der Maßnahme nach Absatz 1 Satz 1 können Personen sein, deren Daten nach § 18 Absatz 1 sowie § 19 Absatz 1 Satz 1 Nummer 2 in der Zentralstelle gespeichert werden dürfen; bei der letztgenannten Personengruppe ist eine besondere Güterabwägung vorzunehmen.

Zu Absatz 3:

Der Abgleich nach Absatz 1 setzt voraus, dass im Informationssystem oder -verbund Daten als Grundlage des Abgleichs vorhanden sind (Beispiele: Lichtbild oder Audioaufnahme eines Tatverdächtigen). Absatz 3 Satz 1 sieht eine entsprechende Geltung des § 12 Absatz 2 für die abzugleichenden Daten vor. Damit werden die Vorgaben der hypothetischen Datenneuerhebung auf die gegenständliche Maßnahme übertragen. Das Bundeskriminalamt darf demnach nur solche Daten in den Abgleich einbeziehen, die mindestens der Verfolgung einer vergleichbar bedeutsamen Straftat dienen und aus denen sich im Einzelfall konkrete Ermittlungsansätze zur Verfolgung solcher Straftaten ergeben. Letzteres sichert, dass nur im Einzelfall notwendige Daten zum Abgleich verwendet werden. Daten, die durch einen verdeckten Einsatz technischer Mittel in oder aus Wohnungen oder verdeckten Eingriff in informationstechnische Systeme erlangt wurden, können aufgrund der hohen Eingriffsintensität nicht in den Abgleich einbezogen werden.

Zu Absatz 4:

Absatz 4 regelt, dass Maßnahmen nach Absatz 1 Satz 1 nur auf Antrag der Präsidentin oder des Präsidenten des Bundeskriminalamts oder ihrer oder seiner Vertretung durch den Ermittlungsrichter angeordnet werden dürfen. Bei Gefahr im Verzug kann die Anordnung auch durch die Präsidentin oder den Präsidenten des Bundeskriminalamts oder ihrer oder seiner Vertretung getroffen werden. Soweit die Anordnung nicht binnen drei Tagen von dem Ermittlungsrichter bestätigt wird, tritt sie außer Kraft.

Die Anordnung kann lediglich als Rechtsgrundlage für einen einzelnen, technisch fehlerfreien Abgleichvorgang dienen. Wiederholte, sich gar einer Echtzeitüberwachung annähernde Such- und Abgleichvorgänge sind nicht zulässig.

Absatz 4 regelt des Weiteren, dass die Anordnung schriftlich zu ergehen hat. Zusätzlich sind konkretisierende Vorgaben für die Entscheidungsformel vorgesehen. In dieser sind nach den Nummern 1 bis 4 anzugeben: Die Person, zu dessen Identifizierung oder Aufenthaltsermittlung die Maßnahme angeordnet wird, die biometrischen Daten aus dem Strafverfahren oder dem Vorgang, die dieser Person zuzuordnen sind, und die zum Abgleich herangezogen werden sollen, und der Tatvorwurf oder Sachverhalt, auf Grund dessen die Maßnahme angeordnet wird.

Zu Absatz 5:

Absatz 5 regelt, dass in der Begründung der Anordnung der Maßnahme deren Voraussetzungen und die wesentlichen Abwägungsgesichtspunkte darzulegen sind. Insbesondere sind einzelfallbezogen die bestimmten Tatsachen, die den Verdacht begründen, die wesentlichen Erwägungen zur Erforderlichkeit und Verhältnismäßigkeit der Maßnahme anzugeben sowie Einzelheiten zur technischen Funktionsweise anzugeben.

Zu Absatz 6:

Die Regelung sichert den Schutz des Kernbereichs privater Lebensgestaltung.

Zu Absatz 7:

Nach Absatz 7 sind die erhobenen und aufbereiteten Daten nach Absatz 1 unverzüglich zu löschen. Nur für den Fall, dass sich auf Grundlage des Abgleichs ein konkreter Ermittlungsansatz aus den Daten ergibt, dürfen diese weiterverarbeitet werden. Dies richtet sich im Weiteren nach den Regelungen zur Weiterverarbeitung nach diesem Gesetz oder der Strafprozessordnung. Die Vorschrift sichert eine enge Zweckbindung der erhobenen Daten.

Zu Absatz 8:

Absatz 8 sieht spezifische Protokollierungsvorgaben vor.

Zu Absatz 9:

Die Regelung in Absatz 9 stellt sicher, dass Dritte im Rahmen einer Auftragsverarbeitung nur tätig werden dürfen, wenn sichergestellt ist, dass die Verarbeitung personenbezogener Daten im Rahmen des Abgleichs nur durch Amtsträger oder für den öffentlichen Dienst besonders Verpflichtete oder zur Geheimhaltung verpflichtete Mitarbeiterinnen oder Mitarbeiter erfolgt. Zudem wird sichergestellt, dass eine Datenverarbeitung stets im Geltungsbereich des EU-Datenschutzregimes stattfindet.

Zu Absatz 10:

Absatz 10 sieht regelmäßige Kontrollpflichten der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit vor.

Zu Absatz 11:

Absatz 11 sieht eine Verordnungsermächtigung vor. Mit der Rechtsverordnung soll das Nähere zu dem technischen Verfahren, den Sicherungsmaßnahmen zur Verhinderung unbefugter Datenzugriffe und, sofern eine Speicherung der abzugleichenden, allgemein öffentlich zugänglichen Lichtbild- Video- und Audiodateien für die Durchführung von Maßnahmen nach Absatz 1 technisch erforderlich ist, nähere Vorgaben zu Art, Umfang und Dauer der Speicherung bestimmt werden. Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit sind hierbei anzuhören.

Zu Nummer 4

Das Bundesverfassungsgericht hat in seinem Urteil vom 16. Februar 2023 zur automatisierten Datenanalyse (Az. 1 BvR 1547/19, 1 BvR 2634/20) die verfassungsrechtliche Legitimität von Befugnissen zur automatisierten Datenanalyse bestätigt und die verfassungsrechtlichen Anforderungen an entsprechende Vorschriften konkretisiert. Die neue Regelung in § 16a setzt diese Anforderungen um.

Die Einrichtung und Nutzung einer automatisierten Anwendung zur Datenanalyse ist für die Aufgabenerfüllung des Bundeskriminalamts erforderlich. Ausgangspunkt ist das der Digitalisierung geschuldete, stetige Ansteigen der vorhandenen Daten, welche durch das Bundeskriminalamt ausgewertet werden müssen. Es bedarf insofern einer Fortentwicklung der technischen Instrumente zur Bewältigung der polizeilichen Aufgaben. Ein Baustein dafür sind Anwendungen zur automatisierten Datenanalyse. Im Vergleich zum Datenabgleich zeichnen sich automatisierte Datenanalysen dadurch aus, dass sie darauf gerichtet sind, neues Wissen zu erzeugen (BVerfG, a. a. O., Randnummer 67).

Das Bundesverfassungsgericht hat in seinem Urteil vom 16. Februar 2023 Kriterien dafür aufgestellt, unter welchen Umständen Eingriffe durch Datenverarbeitungen nicht mehr von den Grundsätzen der Zweckbindung oder hypothetischen Datenneuerhebung gedeckt sind, sondern es eigener Rechtsgrundlagen bedarf. Dazu gehören unter anderem die Fähigkeit der Auswertung großer und komplexer Informationsbestände (BVerfG, a. a. O., Randnummer 69) als auch der Einsatz komplexer Formen des Datenabgleichs (BVerfG, a. a. O., Randnummer 90), wobei es sich jeweils nur um Anhaltspunkte zur Bestimmung der Eingriffsintensität handelt.

Die hier eingeführte Vorschrift ermöglicht es dem Bundeskriminalamt, unter den verfassungsrechtlich zulässigen Voraussetzungen entsprechende Datenanalysen vorzunehmen. Dabei sollen die Datenbestände, die beim Bundeskriminalamt bereits aufgrund bestehender Rechtsgrundlagen rechtmäßig erlangt und gespeichert werden, ausschließlich zum Zwecke der Analyse zusammengeführt und weiterverarbeitet werden.

Das Bundeskriminalamt wird auf diese Weise in die Lage versetzt, bereits bei ihm im polizeilichen Informationssystem oder im polizeilichen Informationsverbund nach § 29 vorhandene Informationen besser, schneller und effizienter auszuwerten. Die Befugnisse zur Weiterverarbeitung von personenbezogenen Daten nach § 16 Absatz

1 und für den (ebenfalls automatisierten) Datenabgleich nach § 16 Absatz 4 bleiben von dieser Regelung unberührt.

Soweit der Anwendungsbereich der Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz) eröffnet ist, gelten die jeweiligen Vorgaben unmittelbar und sind bei der Entwicklung und Nutzung von KI-Systemen zu beachten. Zwingend sicherzustellen ist insbesondere, dass die Rechtskonformität der verwendeten KI-Systeme entsprechend der Verordnung zertifiziert ist. Dies ist in geeigneter Form in der Rechtsverordnung zu konkretisieren. Zur Erprobung von KI-Systemen sollte das Instrument der KI-Reallabore Anwendung finden.

Zu Absatz 1:

Absatz 1 regelt die Befugnis des Bundeskriminalamts, die im Informationssystem des Bundeskriminalamts oder im Informationsverbund gespeicherten Daten mittels einer automatisierten Anwendung zur Datenanalyse aus verschiedenen Datenbeständen technisch zusammenzuführen. Er regelt ferner die Befugnis, diese zusammengeführten Daten zu analysieren, wenn dies zur Erfüllung der Zentralstellenaufgabe des Bundeskriminalamts erforderlich ist. Die besondere verfassungsrechtliche Rolle des Bundeskriminalamts als Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen und für die Kriminalpolizei erfordert hohe Fähigkeiten im Bereich der Auswertung und Analyse von Daten. Als Zentralstelle hat das Bundeskriminalamt insbesondere den gesetzlichen Auftrag, Informationen zu sammeln und auszuwerten und muss daher auch mit den rechtlichen sowie technischen Mitteln ausgestattet werden, die es in die Lage versetzen, diesen Auftrag bestmöglich zu erfüllen.

Voraussetzung ist zunächst, dass dies im Rahmen der Befugnisse des Bundekriminalamts als Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen und für die Kriminalpolizei zur Verfolgung oder Verhütung einer Straftat im Sinne des § 2 Absatz 1 erforderlich ist. Der Einsatz entsprechender Analysen unterliegt einer angemessenen Eingriffsschwelle. Nach dem Urteil des Bundesverfassungsgerichts vom 16. Februar 2023 kann die automatisierte Datenanalyse bei einer hinreichend konkretisierten Gefahr für besonders gewichtige Rechtsgütern erfolgen (BVerfG a. a. O., Randnummer 105f.). Die hohe Schwelle des § 100b Absatz 2 der Strafprozessordnung entspricht diesen Anforderungen an die betroffenen Rechtsgüter. Der Tatbestand 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).

Die technische Zusammenführung der Daten sichert die Verarbeitbarkeit der Daten im Rahmen der automatisierten Datenanalyse. Die Zusammenführung muss aus technischen Gründen vom Einzelfall und weiteren Eingriffsschwellen unabhängig sein. Die Daten können nur dann schnell und effizient analysiert werden, wenn zumindest der Grunddatenbestand bereits zusammengeführt und aktualisiert in einem einheitlichen Datenformat in einer entsprechenden Anwendung vorliegt. Der Vorgang der Zusammenführung und Formatierung ist aufgrund der Masse der Daten aufwändig, so dass eine Zusammenführung lediglich im Einzelfall dem gewünschten Zweck der schnellen und effektiven Gefahrenabwehr nicht gerecht werden könnte.

Die Eingrenzung der Daten auf das Informationssystem nach § 13 und den polizeilichen Informationsverbund nach § 29 ist aus Gründen der Verhältnismäßigkeit angezeigt. Es dürfen lediglich solche Daten einbezogen werden, die bereits rechtmäßig erhoben wurden. Das Bundeskriminalamt wird somit dazu befugt, die automatisierte Analyse interner Datenbestände durchzuführen.

Nicht von der Befugnis umfasst sind Datenerhebungen in externen/öffentlichen Datenquellen wie zum Beispiel Social-Media Plattformen, um diese einer direkten Analyse zu unterziehen. Daten aus externen Quellen können im konkreten Einzelfall in die Analyse nur dann miteinbezogen werden, wenn diese bereits im Vorfeld auf Basis einer entsprechenden Befugnisnorm zur Datenerhebung rechtmäßig erhoben wurden und weiterhin rechtmäßig gespeichert in dem Informationssystem des Bundeskriminalamts vorliegen oder zwischengespeichert werden, ohne dass es zu einer längerfristigen Speicherung der Daten kommt.

Die Vorschrift sieht die automatisierte Datenanalyse des polizeilichen Datenbestands vor. Eine Delegation der Durchführung Datenanalyse an Dritte und eine Übermittlung an diese zu diesem Zweck erlaubt die Vorschrift nicht.

Zu Absatz 2:

Die Zusammenführung und Nutzung automatisierter Anwendungen zur Datenanalyse durch das Bundeskriminalamt ist ebenfalls zur Verhütung von Straftaten gegen Leib, Leben oder Freiheit der nach § 6 zu schützenden Personen erlaubt. Insbesondere die Radikalisierung in der sogenannten Reichsbürger- und Querdenkerszene und die damit verbundene erhöhte Gefährdungslage für die Repräsentanten des Rechtsstaats und der Verfassungsorgane erfordern auch für diesen Aufgabenbereich adäquate rechtliche und technische Fähigkeiten. Aber auch in anderen Phänomenbereichen sind gleichgelagerte Gefahren denkbar.

Der Einsatz entsprechender Analysen unterliegt einer angemessenen Eingriffsschwelle. Nach dem Urteil des Bundesverfassungsgerichts vom 16. Februar 2023 kann die automatisierte Datenanalyse bei einer hinreichend konkretisierten Gefahr für besonders gewichtige Rechtsgütern erfolgen (BVerfG a. a. O., Randnummer 105f.). Darunter fallen die in Absatz 2 Nummer 1 und 2 genannten Rechtsgüter von Leib, Leben und Freiheit. Der Tatbestand 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).

Zu Absatz 3:

Absatz 3 enthält eine nicht abschließende Aufzählung der möglichen Formen der Weiterverarbeitung im Rahmen einer automatisierten Anwendung zur Datenanalyse. Für die Datenverarbeitung sind die in § 12 geregelten Grundsätze zur hypothetischen Datenneuerhebung zu beachten, soweit diese auf die vorliegende Verarbeitungssituation anwendbar sind. Es ist ein ausdrücklicher Verweis auf § 12 Absatz 3 umfasst.

Zu Absatz 4:

Die Regelung stellt eine gesetzliche Sicherung vor den spezifischen Risiken selbstlernender Systeme dar und verpflichtet das Bundeskriminalamt zu technisch-organisatorischen Maßnahmen bei der Verwendung dieser Systeme.

Zu Absatz 5:

Absatz 5 sieht regelmäßige Kontrollpflichten der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit vor.

Zu Absatz 6:

Absatz 6 sieht eine Verordnungsermächtigung vor. Mit der Rechtsverordnung soll das Nähere zu dem technischen Verfahren, den Sicherungsmaßnahmen zur Verhinderung unbefugter Datenzugriffe und nähere Vorgaben zu Art, Umfang und Dauer der Verarbeitung bestimmt werden. Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit sind hierbei anzuhören.

Zu Nummer 5

Zu Buchstabe a

Die Änderung der Überschrift von § 22 folgt aus der Einfügung des Absatzes 3. Eine Aufführung aller Zwecke im Einzelnen ist unübersichtlich, daher wird die Aufzählung im Titel gestrichen.

Zu Buchstabe b

Zu Absatz 3:

Der neue § 22 Absatz 3 schafft eine ausdrückliche Rechtsgrundlage für die Entwicklung, Überprüfung, Änderung und das Trainieren von IT-Produkten durch das Bundeskriminalamt anhand von Echtdaten. IT-Produkte sind entsprechend der Legaldefinition in § 2 Absatz 9a des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) Software, Hardware sowie alle einzelnen oder miteinander verbundenen Komponenten, die Informationen informationstechnisch verarbeiten.

Auch wenn das Testen von IT-Produkten mittels personenbezogener Daten in der Regel eine technisch-organisatorische Maßnahme zur Gewährleistung der Sicherheit der Datenverarbeitung im Produktivbetrieb darstellt, die auf Artikel 6 Absatz 1 Buchstabe c der Verordnung (EU) 2016/679 des Europäischen Parlamentes und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (ABl. L 119/1 vom 4. Mai 2016, S. 1), im Folgenden

Datenschutz-Grundverordnung, in Verbindung mit Artikel 32 der Datenschutz-Grundverordnung beziehungsweise § 64 des Bundesdatenschutzgesetzes gestützt werden kann, soll aus Gründen der Rechtssicherheit eine spezialgesetzliche Rechtsgrundlage geschaffen werden.

Erfüllt das Testen und Trainieren von IT-Produkten im Einzelfall die für die wissenschaftliche Forschung kennzeichnenden Merkmale, ist § 21 als Rechtsgrundlage für die Datenverarbeitung für die wissenschaftliche Forschung heranzuziehen.

Eine Verarbeitung personenbezogener Daten durch das Bundeskriminalamt nach § 22 Absatz 3 Satz 1 ist ausschließlich zum Zwecke der Entwicklung, Überprüfung, Änderung und des Trainierens von IT-Produkten zulässig. Zudem muss es sich um IT-Produkte handeln, die das Bundeskriminalamt für die eigene Aufgabenwahrnehmung entwickelt oder nutzt. Die Datenverarbeitung muss zur Erreichung der benannten Zwecke erforderlich sein. Insbesondere muss ein Bedürfnis für unveränderte Daten bestehen oder eine Anonymisierung oder Pseudonymisierung der Daten nicht oder nur mit unverhältnismäßigem Aufwand möglich sein. Die Aufzählung der Gründe für die Erforderlichkeit der Datenverarbeitung ist nicht abschließend.

Die Regelungen in Absatz 3 Satz 2 und 3 stellen eine gesetzliche Sicherung vor den spezifischen Risken selbstlernende Systeme dar und verpflichtet das Bundeskriminalamt zu technisch-organisatorischen Maßnahmen beim Testen dieser Systeme.

Die Regelungen in Absatz 3 Satz 4 und 5 stellen sicher, dass Dritte im Rahmen einer Auftragsverarbeitung nur tätig werden dürfen, wenn sichergestellt ist, dass die Verarbeitung personenbezogener Daten nur durch Amtsträger oder für den öffentlichen Dienst besonders Verpflichtete oder zur Geheimhaltung verpflichtete Mitarbeiterinnen oder Mitarbeiter erfolgt. Zudem wird sichergestellt, dass eine Datenverarbeitung stets im Geltungsbereich des EU-Datenschutzregimes stattfindet.

Die Regelung in Absatz 3 Satz 6 verbietet die Weiterverarbeitung von Daten nach § 12 Absatz 3 aufgrund der besonders hohen Eingriffsintensität.

Absatz 3 Satz 7 bis 10 entspricht Regelungen in § 21 Absatz 1 Satz 2, Absatz 2 Satz 2, Absatz 4 und 6. Es handelt sich um Schutzregelungen zur zweckkonformen Datenverarbeitung.

Zu Absatz 4:

Absatz 4 sieht eine Verordnungsermächtigung vor. Mit der Rechtsverordnung soll das Nähere zu dem technischen Verfahren, den Sicherungsmaßnahmen zur Verhinderung unbefugter Datenzugriffe und nähere Vorgaben zu Art, Umfang und Dauer der Verarbeitung bestimmt werden. Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit sind hierbei anzuhören.

Zu Nummer 6

Zu Buchstabe a

Zu Doppelbuchstabe aa

Es handelt sich um eine redaktionelle Folgeänderung zur Einfügung von § 33 Absatz 1 Satz 1 Nummer 5.

Zu Doppelbuchstabe bb

Es handelt sich um eine redaktionelle Folgeänderung zur Einfügung von § 33 Absatz 1 Satz 1 Nummer 5.

Zu Doppelbuchstabe cc

Die angefügte Nummer 5 erlaubt die Durchführung eines Abgleichs nach § 10b Absatz 1 zum Zweck der Identifizierung oder Aufenthaltsermittlung, sofern die Voraussetzungen nach § 33 Absatz 1 vorliegen. § 33 Absatz 1 erlaubt Maßnahmen zur Ermittlung des Aufenthaltsorts auf Ersuchen einer zuständigen Behörde eines ausländischen Staates oder eines internationales Strafgerichtshofes. Die Maßnahme nach § 10b Absatz 1 stellt zum Zweck der Identifizierung oder Aufenthaltsermittlung ein vergleichbares Instrument für diesen Zweck dar. Es handelt sich um einen Rechtsfolgenverweis.

Zu Buchstabe b

Zu Doppelbuchstabe aa

Die Ergänzung der neuen Nummer 5 in § 33 Absatz 2 sichert, dass die Maßnahme nur zulässig ist, wenn sie nach deutschem Recht zulässig wäre.

Zu Doppelbuchstabe bb

Die neue Nummer 5 entspricht der Änderung in § 33 Absatz 1 Satz 1 Nummer 5. Auf die Begründung wird insoweit verwiesen. § 33 Absatz 4 erlaubt ebenfalls Maßnahmen zu Ermittlung des Aufenthaltsorts auf Ersuchen von Behörden nach § 26 Absatz 1 und § 27 Absatz 1. Die Maßnahme nach § 10b Absatz 1 fügt sich dementsprechend ein.

Zu Nummer 7

Zum Schutz von Mitgliedern der Verfassungsorgane sind mit Blick auf die terroristische Gefährdungslage im Allgemeinen und die spezifische Bedrohungslage für diesen Personenkreis moderne Ermittlungsmethoden notwendig. Es handelt sich um eine zentrale Aufgabe des Bundeskriminalamts zum Schutz des Staates. Im Übrigen wird auf die Begründung zu § 10b verwiesen.

Zu Artikel 2 (Änderung des Bundespolizeigesetzes)

Zu Nummer 1

Es handelt sich um eine Folgeänderung zu Nummer 3.

Zu Nummer 2

Auf dem Gebiet der Bahnanlagen der Eisenbahnen des Bundes ist für die Abwehr von Gefahren für die Nutzerinnen und Nutzer des Bahnverkehrs sowie die Anlagen des Bahnbetriebs die Bundespolizei zuständig. Die Bundespolizei wird auf Grundlage des neuen § 22 Absatz 1b des Bundespolizeigesetzes tätig, sofern eine Waffenverbotszone nach § 42b Absatz 2 des Waffengesetzes besteht oder eine Allgemeinverfügung, die das Mitführen von Waffen oder bestimmten gefährlichen Gegenständen verbietet. § 22 Absatz 1b ermöglicht es der Bundespolizei, in diesen Bereichen strichprobenartige und anlasslose Kontrollen durchzuführen. Anders lassen sich Führensverbote von Waffen- und Messern nicht effektiv durchsetzen. Insbesondere Messer können verdeckt am Körper getragen werden. Ohne die Möglichkeit einer Durchsuchung der Person würde die Kontrolle und die Durchsetzung von Führensverboten sonst teilweise leerlaufen. Indem Kontrollen jederzeitig und damit für den Betroffenen nicht berechenbar oder planbar durchgeführt werden können, hat dies zugleich eine abstrakt abschreckende Wirkung auf potentielle Täter. Andererseits gilt es zu beachten, dass diese Kontrollen nur in einem räumlich und ggf. auch zeitlich begrenzten Bereich zulässig sind.

Bei Ausübung der Kontrollen hat die zuständige Behörde das ihr obliegende Entschließungsermessen anhand rechtstaatlicher Grundsätze auszuüben. Ob im konkreten Einzelfall vor Ort eine Kontrolle durchgeführt wird, bemisst sich anhand aktueller Lageerkenntnisse im Einzelfall. Ein maßgebliches Kriterium kann dabei u.a. sein, zu welchem Zeitpunkt auf Grund polizeilicher Erkenntnisse mit den meisten Verstößen zu rechnen ist. § 22 Absatz 1b stellt zudem klar, dass die Kontrollen nicht allein an Merkmale im Sinne des Artikels 3 Absatz 3 des Grundgesetzes anknüpfen dürfen. Die Kontrollen sind grundsätzlich anlasslos und stichprobenartig möglich. Ein sachlicher Grund für eine Steuerung der Kontrollen im Einzelfall können aber besondere Lageerkenntnisse sein.

Zu Nummer 3

Zu § 34a:

Die Bundespolizei muss zur Erfüllung ihrer Aufgaben eine wachsende Anzahl von Daten auswerten und miteinander verknüpfen. Dies kann sinnvoll nur über technische Anwendungen geschehen. Der Gesetzentwurf trägt den technischen Möglichkeiten und den Bedarfen der Zeit Rechnung, indem er die Voraussetzung für die Nutzung von Softwares zur automatisierten Datenanalyse durch die Bundespolizei schafft. Bei der konkreten Ausgestaltung wurde den Anforderungen des Bundesverfassungsgerichts im Urteil vom 16. Februar 2023, Az. 1 BvR 1547/19 u. a. Rechnung getragen.

Absatz 1 regelt die Befugnis der Bundespolizei, personenbezogene Daten, die sie zur Erfüllung der ihr obliegenden Aufgaben weiterverarbeitet oder für die sie eine Berechtigung zum Abruf hat, mittels einer automatisierten Anwendung zur Datenanalyse aus verschiedenen Datenbeständen technisch zusammenzuführen. Er regelt ferner die Befugnis, diese zusammengeführten Daten zu analysieren, wenn dies im Rahmen der Aufgaben der Bundespolizei zur Abwehr erheblicher Gefahren erforderlich ist. Hinsichtlich der verfassungsrechtlichen Vorgaben wird auf die Begründung von § 16a des Bundeskriminalamtgesetzes verwiesen. § 34a Absatz 1 Nummer 2 und 3 setzt erhebliche Gefahren im Aufgabenbereich der Bundespolizei voraus.

Zu § 34b:

Entsprechend der Regelung in den §§ 10b und 63b des Bundeskriminalamtgesetzes stellt § 34b eine auf die spezifischen Gefahrenabwehraufgaben der Bundespolizei zugeschnittene Vorschrift dar. Hinsichtlich der Rechtsgüter wird auf die Begründung zu § 34a verwiesen, im Übrigen auf die Begründung zu § 10b des Bundeskriminalamtgesetzes.

Zu Nummer 4

Es handelt sich um eine Verweisanpassung in Folge der Schaffung des § 22 Absatz 1b n.F. Die Norm ergänzt die Befugnis nach § 22 Absatz 1b n.F. Sie schließt insbesondere den Einsatz von Metalldetektoren, Torsonden und ähnlichen technischen Gerätschaften mit ein. Ohne die Möglichkeit einer Durchsuchung würden die Kontrollen nach § 22 Absatz 1b und die Durchsetzung von Waffenverbotszonen oder Allgemeinverfügungen auf dem Gebiet der Eisenbahnen des Bundes teilweise leerlaufen, etwa wenn Waffen und gefährliche Gegenstände verdeckt getragen werden.

Zu Artikel 3 (Änderung der Strafprozessordnung)

Zu Nummer 1

Es handelt sich um eine redaktionelle Folgeänderung zur Einfügung von § 98d.

Zu Nummer 2

Zu Absatz 1

§ 98d StPO-E regelt, unter welchen Voraussetzungen Strafverfolgungsbehörden einen automatisierten biometrischen Abgleich von Lichtbildern oder Audiodateien des Beschuldigten oder einer sonstigen Person, nach der für die Zwecke des Strafverfahrens gefahndet wird, mit Daten im öffentlich zugänglichen Bereich des Internets vornehmen dürfen. Zugrunde gelegt wird die Schwelle des § 100b der Strafprozessordnung. Der Anwendungsbereich betrifft nur den Abgleich mit Lichtbild-, Audio- und Videodateien zur Erkennung des Gesichts und der Stimme. Nicht erfasst ist die Überprüfung von DNA-Merkmalen und sonstigen biometrischen Daten.

Unter allgemein öffentlich zugängliche Daten fallen solche Daten, die von jedermann verwendet werden können, beispielsweise aus sozialen Medien, soweit sich diese nicht an einen spezifisch abgegrenzten Personenkreis richten. Konkretisierend fallen darunter Daten, wenn sie jede Person ohne oder nach vorheriger Registrierung, Genehmigung oder Entgeltzahlung nutzen kann. Nicht umfasst sind Daten, die einer spezifischen Schwelle unterzogen sind, beispielsweise der Einstellung von Daten in sozialen Medien für einen begrenzten Kreis, dessen Zugang einer Kontrolle unterzogen wird. Privatkommunikation über Messenger-Dienste von sozialen Medien können nicht von der Maßnahme erfasst werden

Zu Satz 1

Zu Nummer 1

§ 98d Absatz 1 Satz 1 Nummer 1 StPO-E regelt entsprechend § 100b Absatz 1 Nummer 1 StPO, dass für den automatisierten biometrischen Abgleich von Lichtbildern und Audioaufzeichnungen eines Beschuldigten oder einer sonstigen Person, nach der für die Zwecke des Strafverfahrens gefahndet wird, mit Daten im öffentlich zugänglichen Bereich des Internets bestimmte Tatsachen den Verdacht begründen müssen, dass jemand als Täter oder Teilnehmer eine in § 100b Absatz 2 StPO bezeichnete schwere Straftat begangen, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht, oder durch eine Straftat vorbereitet hat.

Zu Nummer 2

§ 98d Absatz 1 Satz 1 Nummer 2 StPO-E regelt entsprechend § 100b Absatz 1 Nummer 2 StPO als kumulative Voraussetzung zu Nummer 1, dass die Tat auch im Einzelfall schwer wiegen muss.

Zu Nummer 3

§ 98d Absatz 1 Satz 1 Nummer 3 StPO-E regelt entsprechend § 100b Absatz 1 Nummer 3 StPO als weitere kumulative Voraussetzung ausdrücklich den Subsidiaritätsgrundsatz. Eine Maßnahme nach § 98d Absatz 1 Satz 1 StPO soll erst dann in Betracht kommen, wenn die Identitätsfeststellung oder die Ermittlung des Aufenthaltsortes des Beschuldigten oder der sonstigen Person, nach der für die Zwecke des Strafverfahrens gefahndet wird, auf andere Weise wesentlich erschwert oder aussichtslos wäre.

Zu Satz 2

Mit § 98d Absatz 1 Satz 2 wird klargestellt, dass ein Abgleich mit biometrischen Daten aus im Internet öffentlich zugänglichen Echtzeit-Lichtbild- und Echtzeit-Videodateien ausgeschlossen ist, damit hierüber keine Echtzeitüberwachung bestimmter Bereiche stattfinden kann. Erfasst hiervon sind insbesondere Live-Streams, zum Beispiel von Veranstaltungen, in denen auch das Publikum erfasst wird, oder das Live-Video einer Webcam eines öffentlich zugänglichen Ortes. Ausdrücklich erfasst sind auch Echtzeit-Lichtbild-Dateien, also beispielsweise die Bilder von Webcams, die in zeitlich kurzer Abfolge einzelne Lichtbilder ins Internet hochladen.

Zu Absatz 2

§ 98d Absatz 2 StPO-E regelt, dass Maßnahmen nach Absatz 1 nur auf Antrag der Staatsanwaltschaft durch den Ermittlungsrichter angeordnet werden dürfen. Bei Gefahr im Verzug kann die Anordnung auch durch die Staatsanwaltschaft getroffen werden. Soweit die Anordnung der Staatsanwaltschaft nicht binnen drei Tagen von dem Ermittlungsrichter bestätigt wird, tritt sie außer Kraft.

Die Anordnung kann lediglich als Rechtsgrundlage für einen einzelnen, technisch fehlerfreien Abgleichvorgang dienen. Wiederholte, sich gar einer Echtzeitüberwachung annähernde Such- und Abgleichvorgänge sind nicht zulässig. § 98d Absatz 2 Satz 4 StPO-E regelt, dass die Anordnung schriftlich zu ergehen hat. Zusätzlich sind nach dem Vorbild der Vorgaben aus § 100e Absatz 3 StPO in Satz 5 konkretisierende Vorgaben für die Entscheidungsformel vorgesehen. In dieser sind nach den Nummern 1 bis 3 anzugeben: Die Person, zu dessen Identifizierung oder Aufenthaltsermittlung die Maßnahme angeordnet wird, die biometrischen Daten aus dem Strafverfahren, die dieser Person zuzuordnen sind, und die zum Abgleich herangezogen werden sollen, und der Tatvorwurf, auf Grund dessen die Maßnahme angeordnet wird. Damit wird schon mit dem Entscheidungssatz gewährleistet, dass die Maßnahme inhaltlich den Anforderungen an die betroffenen Grundrechte genügt.

Zu Absatz 3

§ 98d Absatz 3 StPO-E regelt, dass in der Begründung der Anordnung der Maßnahme deren Voraussetzungen und die wesentlichen Abwägungsgesichtspunkte darzulegen sind. Insbesondere sind einzelfallbezogen die bestimmten Tatsachen, die den Verdacht begründen, die wesentlichen Erwägungen zur Erforderlichkeit und Verhältnismäßigkeit der Maßnahme sowie zur technischen Funktionsweise anzugeben.

Zu Absatz 4

Der biometrische Abgleich von Daten aus dem Internet zu Fahndungszwecken mit anderen Datenbeständen ist mit Eingriffen in die informationelle Selbstbestimmung verbunden. Von dem Abgleich können auch solche Lichtbild- und Videodateien erfasst sein, die gegen oder ohne das Einverständnis des Betroffenen von Dritten ins Internet übertragen werden oder Informationen unfreiwillig preisgeben. Bei der Intensität des Eingriffs ist auch zu berücksichtigen, dass der Abgleich auch mittels eines KI-Systems erfolgen kann. Es sind daher die Kernbereichsregelungen entsprechend anzuwenden, die § 100d Absatz 1 bis 3 bereits für andere eingriffsintensive Maßnahmen vorsieht.

Zu Absatz 5

§ 98d Absatz 5 Satz 1 StPO-E regelt in Ergänzung zu § 101 Absatz 8 StPO, dessen Anwendungsbereich mit Artikel 3 Nummer 3 auf § 98d StPO-E erstreckt wird, dass die im Rahmen des Abgleichs nach Absatz 1 erhobenen Daten nach Durchführung des Abgleichs nicht nur dann unverzüglich zu löschen sind, wenn sie für die Strafverfolgung nicht mehr erforderlich sind, sondern bereits dann, wenn sie keinen konkreten Ermittlungsansatz für die Aufenthaltsermittlung oder Identifizierung der Zielperson aufweisen. Dies soll verhindern, dass die zum Abgleich

herangezogenen Daten länger als für den Abgleich und die Aufenthaltsermittlung oder Identifizierung der Zielperson nötig gespeichert werden. Satz 2 bestimmt in Ergänzung zu § 101 Abs. 8 StPO, dass dies auch für sonstige erhobene Daten gilt, soweit schutzwürdige Interessen des Betroffenen im Einzelfall gegenüber dem Strafverfolgungsinteresse überwiegen.

§ 98d Absatz 5 Satz 3 StPO-E bestimmt, dass im Falle des Absatz 2 Satz 3 alle bereits erhobenen Daten unverzüglich zu löschen sind. Wenn die Anordnung durch die Staatsanwaltschaft wegen fehlendem Vorliegen der Eingriffsvoraussetzungen nicht durch das Gericht bestätigt wird, sollen auch die Daten gelöscht werden, die einen Ermittlungsansatz beinhalten, da diese dann rechtswidrig erlangt wurden. Nach § 98d Absatz 5 Satz 3 StPO-E soll – wie bei § 100d Absatz 2 Satz 3 StPO – die Löschung aktenkundig gemacht werden.

Zu Absatz 6

§ 98d Absatz 6 Satz 1 StPO-E regelt, dass bei jeder Maßnahme die konkret eingesetzte automatisierten Anwendung zur Datenverarbeitung, der Zeitpunkt ihres Einsatzes und die Organisationseinheit, die die Maßnahme durchführt, zu protokollieren ist. Damit soll eine Überprüfung ermöglicht werden, ob dem Suchlauf ein entsprechender gerichtlicher Beschluss zugrunde lag. Die Regelung bezüglich der Bezeichnung der eingesetzten Software soll der Transparenz dienen. Gemäß § 98d Absatz 6 Satz 2 StPO-E soll nach Beendigung einer Maßnahme die Stelle unterrichtet werden, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz bei öffentlichen Stellen zuständig ist. Satz 2 entspricht § 98b Absatz 4 StPO.

Mit der Anzeigepflicht nach § 98d Absatz 6 Satz 2 und der Pflicht, nach § 98d Absatz 6 Satz 1 zu dokumentieren, welches System eingesetzt wird, ist sichergestellt, dass der zuständige Landes- oder Bundesbeauftragte für den Datenschutz bereits unmittelbar nach Beendigung des erstmaligen Einsatzes hiervon – und damit von der Einführung eines solchen Systems an sich – erfährt. Er kann dann seine ihm zustehenden Befugnisse ausüben, zum Beispiel im Bereich der Zuständigkeit des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit das Recht zur Beanstandung gegenüber der zuständigen obersten Bundesbehörde bei Vorliegen von Verstößen oder Mängeln im Zusammenhang mit Datenschutzvorschriften. Zudem besteht die Möglichkeit zur Warnung, wenn solche Verstöße voraussichtlich drohen (vgl. § 16 Absatz 2 Satz 1 und 4 Bundesdatenschutzgesetz – BDSG).

Darüber hinaus ist nach geltendem Recht bei der Verwendung neuer Technologien – bereits vor ihrem Einsatz – teilweise die Durchführung einer Datenschutz-Folgenabschätzung vorgesehen. Für den Bereich des Bundes ergibt sich dies aus § 500 StPO in Verbindung mit § 67 BDSG. Gemäß § 67 Absatz 3 BDSG haben die Verantwortlichen den zuständigen Datenschutzbeauftragten der öffentlichen Stelle an der Durchführung der Folgenabschätzung zu beteiligen. Auch in Landesgesetzen finden sich solche Bestimmungen. So schreibt etwa § 62 des Hessischen Datenschutz- und Informationsfreiheitsgesetzes ebenfalls die Durchführung einer Datenschutz-Folgenabschätzung vor.

Zu Absatz 7

Die Regelung in Absatz 7 stellt sicher, dass Dritte im Rahmen einer Auftragsverarbeitung nur tätig werden dürfen, wenn sichergestellt ist, dass die Verarbeitung personenbezogener Daten im Rahmen des Abgleichs nur durch Amtsträger oder für den öffentlichen Dienst besonders Verpflichtete oder zur Geheimhaltung verpflichtete Mitarbeiterinnen oder Mitarbeiter erfolgt. Zudem wird sichergestellt, dass eine Datenverarbeitung stets im Geltungsbereich des EU-Datenschutzregimes stattfindet.

Zu Absatz 8

Absatz 8 sieht eine Verordnungsermächtigung vor. Mit der Rechtsverordnung soll das Nähere zu dem technischen Verfahren, den Sicherungsmaßnahmen zur Verhinderung unbefugter Datenzugriffe und, sofern eine Speicherung der abzugleichenden, allgemein öffentlich zugänglichen Lichtbild- Video- und Audiodateien für die Durchführung von Maßnahmen nach Absatz 1 technisch erforderlich ist, nähere Vorgaben zu Art, Umfang und Dauer der Speicherung bestimmt werden. Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit sind hierbei anzuhören. Die Rechtsverordnung bedarf der Zustimmung des Bundesrates (vgl. Artikel 80 Absatz 2 des Grundgesetzes).

Zu Nummer 3

Zu Buchstabe a

§ 101 StPO trifft Verfahrensregelungen für verdeckte Maßnahmen. § 98d StPO-E wird in die Aufzählung der heimlichen Maßnahmen aufgenommen, sodass die Verfahrensregelungen auch hier unmittelbare Anwendung finden. Dies umfasst insbesondere Regelungen zu Kennzeichnungs- (§ 101 Absatz 3 StPO) und Benachrichtigungspflichten (§ 101 Absatz 4 bis 7 StPO; vgl. dazu auch die Änderung unter Buchstabe b).

Auch Lösch- und Einschränkungspflichten nach § 101 Absatz 8 StPO sind zu beachten: Nach dieser Vorschrift sind die durch die Maßnahme erlangten personenbezogenen Daten unverzüglich zu löschen, sofern sie zur Strafverfolgung und für eine etwaige gerichtliche Überprüfung der Maßnahme nicht mehr erforderlich sind. Dies gilt unter anderem dann, wenn Treffer keinen konkreten Ansatz für die Ermittlung der Identität oder des Aufenthalts aufweisen. Das Löschgebot ist aber auch einschlägig, wenn sich nach einem Treffer die vermutete Identität des Betroffenen bestätigen lässt durch den Abgleich mit einer anderen Quelle, etwa durch Abruf seines Lichtbilds aus dem Personalausweisregister. Die Löschvorschrift stellt so sicher, dass Bild-, Audio- und Videomaterial des Betroffenen – das regelmäßig keinen Bezug zum konkreten Strafverfahren hat – nur so lange in den Unterlagen der Strafverfolgungsbehörden verbleibt, wie dies zur Identitätsfeststellung oder Aufenthaltsermittlung nötig ist. Den schutzwürdigen Interessen der Betroffenen wird so weitestmöglich Rechnung getragen.

Zu Buchstabe b

§ 101 Absatz 4 Satz 1 StPO regelt, welche Personen bei welchen verdeckten Maßnahmen zu benachrichtigen sind. In den Katalog wird neu Nummer 1a aufgenommen, der für eine Maßnahme nach § 98d StPO-E bestimmt, dass die Person, zu deren Identifizierung oder Aufenthaltsermittlung die Maßnahme angeordnet wird, zu benachrichtigen ist.

Zu Artikel 4 (Evaluierung)

Der fachunabhängigen wissenschaftlichen Einrichtung, die die Anwendung der Vorschriften evaluiert, sind die für die Erledigung des Auftrags erforderlichen Informationen zur Verfügung zu stellen. Dazu gehören insbesondere statistische Informationen über Häufigkeit und Dauer der Maßnahmen, detaillierte Einblicke in die Funktionsweise und konkrete Nutzung der eingesetzten Systeme sowie in Leitfäden und Verfahrensvorschriften, in einzelne Verfahrensakten sowie eine teilnehmende Beobachtung bei Durchführung der Maßnahmen. Sofern notwendig sind die beteiligten Einrichtungen und Personen auf geeignete Weise zur Geheimhaltung zu verpflichten.

Die Evaluierung ist mit der Evaluierung der Anwendung von § 15b des Asylgesetzes zu verbinden.

Zu Artikel 5 (Inkrafttreten)

Die Bestimmung regelt das Inkrafttreten des Gesetzes.