Bundesrat **Drucksache** **264/26**

01.05.26

R - Fz - In

Gesetzentwurf
der Bundesregierung

Entwurf eines Gesetzes zur Änderung der Strafprozessordnung - digitale Ermittlungsmaßnahmen

A. Problem und Ziel

Der Entwurf verfolgt das Ziel, Strafverfolgungsbehörden mit neuen Befugnissen auszustatten, um die Effektivität der Strafverfolgung zu steigern.

Bislang gibt es keine ausdrückliche Ermächtigungsgrundlage, die den automatisierten Abgleich biometrischer Daten aus einem Strafverfahren mit im Internet öffentlich zugänglichen Daten regelt. Daher dürfen die Ermittlungsbehörden einen solchen Abgleich derzeit nur manuell, also ohne den Einsatz einer speziellen, für den Abgleich entwickelten Software, unter Einsatz gängiger Internet-Suchmaschinen, vornehmen, um Personen zu identifizieren, lokalisieren oder Tat-Täter-Zusammenhänge zu erschließen. Dies kann insbesondere im Falle großer Datenmengen im Einzelfall zur Erfolglosigkeit von Ermittlungsmaßnahmen führen und außerdem in erheblichem Umfang Personal der Strafverfolgungsbehörden binden. Aus der am 1. August 2024 in Kraft getretenen Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rats 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) (ABl. L, 2024/1689, 12.7.2024) ergibt sich die Notwendigkeit, spezielle Regelungen für den Einsatz von Systemen künstlicher Intelligenz im Sinne von Artikel 3 Nummer 1 (KI-Systeme) zu schaffen, wenn sie zur biometrischen Fernidentifizierung eingesetzt werden sollen.

Gegenwärtig gibt es auch keine Ermächtigungsgrundlage für den Einsatz verfahrensübergreifender Recherche- und Analyseplattformen zur Strafverfolgung. Das Bundesverfassungsgericht hat in dem zur Gefahrenabwehr ergangenen Urteil vom 16. Februar 2023 – 1 BvR 1547/19, 1 BvR 2634/20 – deutlich gemacht, dass deren Nutzung einer ausdrücklichen Ermächtigungsgrundlage bedarf. Derzeit beruht die operative IT-Infrastruktur der Polizeibehörden teilweise noch auf einem unverbundenen Nebeneinander zahlreicher automatisierter Dateien und Datenquellen, die zur Strafverfolgung noch jeweils einzeln mit einem bestimmten personenbezogenen Datum abgeglichen werden müssen. Dies bindet zum einen personelle Ressourcen, zum anderen birgt dies ein Risiko von Übertragungsfehlern, Informationsverlusten oder paralleler Datenhaltung, zumal jede neue Fragestellung erneut unter den vorangestellten Einschränkungen und Aufwänden bearbeitet werden muss. Mit dem Einsatz verfahrensübergreifender Recherche- und Analyseplattformen

---

Fristablauf: 12.06.26

Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln
Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.bundesanzeiger-verlag.de
ISSN 0720-2946

könnten bisher unverbundene Dateien und Datenquellen der Polizei, die sowohl die Daten aus der Gefahrenabwehr als auch aus der Strafverfolgung enthalten, in einer Analyseplattform vernetzt werden und durch Suchfunktionen systematisch erschlossen und analysiert werden.

B. Lösung

Für den automatisierten Abgleich biometrischer Daten aus einem Strafverfahren mit biometrischen Daten aus im Internet öffentlich zugänglichen Daten soll eine klare Rechtsgrundlage geschaffen werden. Des Weiteren wird den Strafverfolgungsbehörden die Befugnis eingeräumt, zur Strafverfolgung verfahrensübergreifende Recherche- und Analyseplattformen einzusetzen.

C. Alternativen

Keine.

D. Haushaltsausgaben ohne Erfüllungsaufwand

Es entstehen in den Haushalten des Bundes und der Gemeinden keine Haushaltsausgaben ohne Erfüllungsaufwand.

In den Haushalten der Länder entsteht voraussichtlich ein Mehrbedarf an Stellen, Personal- und Sachkosten. Sämtliche Länder gaben an, die Mehrbedarfe nicht belastbar schätzen zu können.

E. Erfüllungsaufwand

E.1 Erfüllungsaufwand für Bürgerinnen und Bürger

Keiner.

E.2 Erfüllungsaufwand für die Wirtschaft

Keiner.

Davon Bürokratiekosten aus Informationspflichten

Keine.

E.3 Erfüllungsaufwand der Verwaltung

Keiner.

F. Weitere Kosten

Für die Strafverfolgungsbehörden der Länder eröffnen die neuen Befugnisse die Möglichkeit, die technischen Voraussetzungen für den biometrischen Internetabgleich und die automatisierte Datenanalyse einzuführen und diese Maßnahmen anzuwenden. In diesem Fall ist von einem Mehraufwand auszugehen, der von den Ländern derzeit noch nicht beziffert werden konnte. Dieser entsteht aufgrund der Notwendigkeit der Softwarebeschaffung, Weiterentwicklung und des Weiterbetriebes sowie durch weitere sächliche und

personelle Aufwände, wie etwa für Schulungen des mit den Maßnahmen beauftragten Personals. Bei Ländern, die heute schon im Bereich der Gefahrenabwehr Software für eine automatisierte Datenanalyse einsetzen, ist zu erwarten, dass keine neue Software angeschafft, aber vorhandene an die Vorgaben der Nutzung für die Strafverfolgung anzupassen ist. Auf der anderen Seite ist von kostenrelevanten Effektivitätsgewinnen auszugehen, denn es ist zu erwarten, dass durch die Anwendung der Maßnahmen aufwendigere alternative, händische Ermittlungsmaßnahmen in konkreten Ermittlungsverfahren vermieden werden können. In welcher Höhe sich Einsparpotentiale realisieren lassen, konnte von den Ländern ebenfalls nicht belastbar geschätzt werden.

Für den Generalbundesanwalt beim Bundesgerichtshof, das Bundeskriminalamt und die Bundespolizei sind infolge der neuen strafprozessualen Befugnisse keine zusätzlichen Kosten zu erwarten.

Bundesrat **Drucksache** **264/26**

01.05.26

R - Fz - In

Gesetzentwurf
der Bundesregierung

Entwurf eines Gesetzes zur Änderung der Strafprozessordnung - digitale Ermittlungsmaßnahmen

Bundesrepublik Deutschland
Der Bundeskanzler

Berlin, 1. Mai 2026

An den
Präsidenten des Bundesrates
Herrn Bürgermeister
Dr. Andreas Bovenschulte

Sehr geehrter Herr Bundesratspräsident,

hiermit übersende ich gemäß Artikel 76 Absatz 2 des Grundgesetzes den von der Bundesregierung beschlossenen

> Entwurf eines Gesetzes zur Änderung der Strafprozessordnung –
> digitale Ermittlungsmaßnahmen

mit Begründung und Vorblatt.

Federführend ist das Bundesministerium der Justiz und für Verbraucherschutz.

Mit freundlichen Grüßen
Friedrich Merz

Fristablauf: 12.06.26

Entwurf eines Gesetzes zur Änderung der Strafprozessordnung – digitale Ermittlungsmaßnahmen

Vom ...

Der Bundestag hat das folgende Gesetz beschlossen:

Artikel 1

Änderung der Strafprozessordnung

Die Strafprozessordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch Artikel 2 Absatz 7 des Gesetzes vom 20. März 2026 (BGBl. 2026 I Nr. 95) geändert worden ist, wird wie folgt geändert:

1. In der Inhaltsübersicht wird nach der Angabe zu § 98c die folgende Angabe eingefügt:

   „§ 98d Automatisierter biometrischer Abgleich mit öffentlich zugänglichen Daten aus dem Internet

   § 98e Automatisierte verfahrensübergreifende Datenanalyse“.

2. Nach § 98c werden die folgenden §§ 98d und 98e eingefügt:

„§ 98d

Automatisierter biometrischer Abgleich mit öffentlich zugänglichen Daten aus dem Internet

(1) Zur Erforschung des Sachverhalts, zur Identitätsfeststellung oder zur Ermittlung des Aufenthaltsorts des Beschuldigten oder eines Zeugen dürfen biometrische Daten aus einem Strafverfahren mit im Internet öffentlich zugänglichen biometrischen Daten mittels einer automatisierten Anwendung zur Datenverarbeitung abgeglichen werden, wenn

1. bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Absatz 2 bezeichnete Straftat, begangen hat, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat oder durch eine Straftat vorbereitet hat und,

2. die Erforschung des Sachverhalts, die Identitätsfeststellung oder die Ermittlung des Aufenthaltsortes auf andere Weise wesentlich erschwert oder aussichtslos wäre.

Ein Abgleich mit öffentlich zugänglichen Echtzeitdaten ist unzulässig.

(2) Bei jedem Abgleich sind zu protokollieren:

1. die Bezeichnung der automatisierten Anwendung zur Datenverarbeitung und der Zeitpunkt ihres Einsatzes,

2. Angaben, die die Feststellung der erhobenen Daten ermöglichen, und

3. die Organisationseinheit, die die Maßnahme durchführt.

(3) Die beim Abgleich erhobenen und verarbeiteten Daten sind nach Durchführung des Abgleichs unverzüglich zu löschen, soweit sie keinen konkreten Ermittlungsansatz für das Verfahren oder ein anderes Strafverfahren aufweisen. Die Löschung ist aktenkundig zu machen.

(4) Der Abgleich wird durch die Staatsanwaltschaft angeordnet. Bei Gefahr im Verzug dürfen auch Ermittlungspersonen der Staatsanwaltschaft (§ 152 des Gerichtsverfassungsgesetzes) den Abgleich anordnen; in diesem Fall ist die Entscheidung durch die Staatsanwaltschaft unverzüglich, spätestens aber binnen 48 Stunden, herbeizuführen.

§ 98e

Automatisierte verfahrensübergreifende Datenanalyse

(1) Begründen bestimmte Tatsachen den Verdacht, dass jemand als Täter oder Teilnehmer eine auch im Einzelfall schwerwiegende, in § 100a Absatz 2 bezeichnete schwere Straftat begangen hat, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat oder durch eine Straftat vorbereitet hat, dürfen zur Aufklärung dieser Straftat oder zur Ermittlung des Aufenthalts einer Person, nach der für die Zwecke des Strafverfahrens gefahndet wird, in Datei- und Informationssystemen der Polizei rechtmäßig gespeicherte und für eine polizeiliche Analyseplattform zusammengeführte personenbezogene Daten mittels einer automatisierten Anwendung zur Datenverarbeitung weiterverarbeitet werden.

(2) Bei der Weiterverarbeitung dürfen Vorgangsdaten, Falldaten, Daten aus den polizeilichen Informationssystemen und aus dem polizeilichen Informationsaustausch einbezogen werden. Die aufgrund von Maßnahmen nach den §§ 100a, 100f, 100g, 100k Absatz 1 und 2, § 100i in anderen Strafverfahren oder entsprechenden Maßnahmen nach anderen Gesetzen gewonnenen sowie die aus Asservaten stammenden personenbezogenen Daten dürfen ergänzend einbezogen werden, soweit dies erforderlich ist. Die aufgrund von Maßnahmen nach den §§ 100b und 100c in anderen Strafverfahren oder entsprechenden Maßnahmen nach anderen Gesetzen erlangten personenbezogenen Daten dürfen nicht einbezogen werden.

(3) Eine direkte Anbindung der Analyseplattform an sonstige, nicht-polizeiliche Register und an Internetdienste ist unzulässig. Datensätze aus gezielten, auch automatisierten Abfragen in sonstigen staatlichen Registern und im Einzelfall erhobene Datensätze aus Internetquellen können in die Weiterverarbeitung einbezogen werden.

(4) Im Rahmen der Weiterverarbeitung können basierend auf dem Abgleich personenbezogener Daten

1. datei- und informationssystemübergreifend Beziehungen oder Zusammenhänge zwischen Verfahren, Vorgängen, Personen, Personengruppierungen, Institutionen, Organisationen, Orten, Objekten und Sachen identifiziert und hergestellt, sowohl qualitativ als auch quantitativ klassifiziert, strukturell analysiert und visualisiert werden,

2. für die Erreichung des Zwecks der Weiterverarbeitung unbedeutende Informationen und Erkenntnisse ausgeschlossen werden,

3. eingehende Erkenntnisse zu bekannten Sachverhalten zugeordnet werden,

4. Suchkriterien, insbesondere nach Sachnähe, Aktualität und Erheblichkeit der Verknüpfung mit anderen Informationen bezogen auf den Zweck der Weiterverarbeitung nach Absatz 1, gewichtet werden sowie

5. gespeicherte Daten statistisch ausgewertet werden.

Die Methodik der automatisierten Anwendung zur Datenverarbeitung hat sich darauf zu beschränken, Daten aufzubereiten und bereitzustellen, die es den Strafverfolgungsbehörden ermöglichen, eigene Bewertungen und Entscheidungen zu treffen. Jeder Einsatz der Anwendung muss anlassbezogen und manuell ausgelöst werden und anhand von Suchbegriffen erfolgen, die sich aus einem konkreten Sachverhalt ergeben. Eine ausschließlich auf der Maßnahme nach Absatz 1 beruhende automatisierte Entscheidungsfindung, die unmittelbar eine nachteilige Rechtsfolge für die betroffene Person hat oder diese erheblich beeinträchtigt, ist unzulässig. Es ist technisch und organisatorisch sicherzustellen, dass diskriminierende Algorithmen weder herausgebildet noch verwendet werden.

(5) Der Einsatz der automatisierten Anwendung zur Datenverarbeitung ist unter Darlegung der Voraussetzungen nach Absatz 1, bei Einbeziehung von Daten nach Absatz 2 Satz 2 auch unter Darlegung der hierfür geltenden Voraussetzungen, zu begründen. § 98d Absatz 2 gilt entsprechend.

(6) Im Übrigen bleibt das für die speichernde Stelle geltende Recht über die Verarbeitung personenbezogener Daten und die Rechte der Betroffenen einschließlich der Übermittlungsvorschriften und Verwendungsregelungen unberührt. Dessen Einhaltung ist technisch und organisatorisch sicherzustellen.“

3. § 101 wird wie folgt geändert:

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

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

„1a. des § 98d die Person, deren biometrische Daten aus dem Strafverfahren für einen Abgleich nach § 98d verwendet wurden,“.

Artikel 2

Inkrafttreten

Dieses Gesetz tritt am Tag nach der Verkündung in Kraft.

Begründung

A. Allgemeiner Teil

I. Zielsetzung und Notwendigkeit der Regelungen

Der Entwurf verfolgt das Ziel, Strafverfolgungsbehörden mit neuen Befugnissen auszustatten, um die Effektivität der Strafverfolgung zu steigern.

Bislang gibt es keine ausdrückliche Ermächtigungsgrundlage, die den automatisierten Abgleich von biometrischen Daten aus einem Strafverfahren mit im Internet öffentlich zugänglichen Daten regelt. Nach geltender Rechtslage können im Internet öffentlich zugängliche biometrische Daten als sogenannte Open-Source-Intelligence-Maßnahme (OSINT-Maßnahme) manuell, also ohne den Einsatz einer speziellen, für den Abgleich entwickelten Software, unter Einsatz gängiger Internet-Suchmaschinen auf Grundlage der Ermittlungsgeneralklauseln der §§ 161, 163 der Strafprozessordnung (StPO) mit personenbezogenen Daten, insbesondere biometrischen Daten aus einem Strafverfahren zur Sachverhaltsaufklärung abgeglichen werden (vergleiche Wabnitz/Janovsky/Schmitt WirtschaftsStrafR-HdB/Bär, 6. Auflage 2025, Kap. 30 Rn. 123 f., beck-online; KK-StPO/Weingarten, 9. Auflage 2023, StPO § 161 Rn. 12a, beck-online). Allein die Kenntnisnahme von im Internet öffentlich zugänglichen Informationen bewirkt in aller Regel keinen Grundrechtseingriff (vergleiche BVerfG, Urteil vom 27. 2. 2008 – 1 BvR 370/07, 1 BvR 595/07 – Rn. 298). Anders ist dies, wenn hierfür automatisierte Anwendungen zur Datenverarbeitung eingesetzt werden, da hier mit Blick auf die potentielle Menge der abzugleichenden Daten potentiell viele Unbeteiligte betroffen sein dürften.

Aus der am 1. August 2024 in Kraft getretenen Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rats 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) (ABl. L, 2024/1689, 12.7.2024) ergibt sich zudem die Notwendigkeit, für Systeme künstlicher Intelligenz im Sinne von Artikel 3 Nummer 1 (KI-Systeme) spezielle Regelungen zu schaffen, wenn der Einsatz von KI-Systemen zur biometrischen Fernidentifizierung vorgesehen ist.

Für den automatisierten Abgleich biometrischer Daten aus einem Strafverfahren mit biometrischen Daten aus im Internet öffentlich zugänglichen Daten wird daher eine ausdrückliche Rechtsgrundlage geschaffen.

Des Weiteren wird den Strafverfolgungsbehörden die Befugnis eingeräumt, zur Strafverfolgung verfahrensübergreifende Recherche- und Analyseplattformen einzusetzen. Mit dem Einsatz verfahrensübergreifender Recherche- und Analyseplattformen zur Strafverfolgung können bisher unverbundene Dateien und Datenquellen der Polizei, die sowohl die Daten aus der Gefahrenabwehr als auch aus der Strafverfolgung enthalten, in einer Analyseplattform vernetzt werden und durch Suchfunktionen systematisch erschlossen werden. Aufgesetzt werden soll auf bereits vorhandene Analyseplattformen der Gefahrenabwehr.

Derzeit beruht die operative IT-Infrastruktur der Polizeibehörden teilweise noch auf einem unverbundenen Nebeneinander zahlreicher automatisierter Dateien und Datenquellen, die zur Strafverfolgung noch jeweils einzeln mit einem bestimmen personenbezogenen Datum abgeglichen werden müssen. Dies bindet zum einen personelle Ressourcen, zum anderen birgt dies ein Risiko von Übertragungsfehlern, Informationsverlusten oder paralleler

Datenhaltung, zumal jede neue Fragestellung erneut unter den vorangestellten Einschränkungen und Aufwänden bearbeitet werden muss (vergleiche zur Gefahrenabwehr, Drucksache des Bayerischen Landtags 19/1557, Seite 12). Dies kann im Einzelfall dazu führen, dass wesentliche Anhaltspunkte für die Aufklärung der konkreten Straftat entweder nur mit hohem Personal- und Zeitaufwand gewonnen werden können oder dass sie überhaupt nicht erkannt werden (vergleiche auch zur Gefahrenabwehr Drucksache des Landtags Rheinland-Pfalz 18/10756, Seite 2). Dies soll der Einsatz verfahrensübergreifender Analyseplattformen überwinden. Diese können es ermöglichen, eine Vielzahl von für die Aufklärung der konkreten Straftat relevanten, personenbezogenen Daten in mehrfachen, automatisierten Schritten mit einer Vielzahl von Quellsystemen auf einmal abzugleichen und hierdurch in kurzer Zeit datei- und informationssystemübergreifend Beziehungen oder Zusammenhänge zwischen Personen, Personengruppierungen, Institutionen, Organisationen, Orten, Objekten und Sachen herzustellen und graphisch darzustellen.

Gegenwärtig gibt es keine Ermächtigungsgrundlage für den Betrieb von verfahrensübergreifenden Recherche- und Analyseplattformen zur Strafverfolgung. Eine datei- und informationssystemübergreifende Zusammenführung und komplexe Analyse dieser zusammengeführten Daten ist nicht von § 98c StPO erfasst. § 98c StPO ermöglicht nur einen einfachen maschinellen Datenabgleich. Das Bundesverfassungsgericht hat in dem zur Gefahrenabwehr ergangenen Urteil vom 16. Februar 2023 – 1 BvR 1547/19, 1 BvR 2634/20 – (Palantir) deutlich gemacht, dass die Nutzung von Analyseplattformen einer ausdrücklichen Ermächtigungsgrundlage bedarf.

II. Wesentlicher Inhalt des Entwurfs

Mit § 98d der Strafprozessordnung in der Entwurfsfassung (StPO-E) wird eine Ermächtigungsgrundlage für den automatisierten Abgleich biometrischer Daten aus einem Strafverfahren mit im Internet öffentlich zugänglichen Daten geschaffen. Zweck der Maßnahme kann die Erforschung des Sachverhalts, die Identitätsfeststellung oder die Ermittlung des Aufenthaltsorts des Beschuldigten oder eines Zeugen sein.

§ 98e StPO-E regelt die Befugnis der Strafverfolgungsbehörden, zur Aufklärung einer Straftat oder zur Ermittlung des Aufenthalts einer Person, nach der für die Zwecke des Strafverfahrens gefahndet wird, in Datei- und Informationssystemen der Polizei rechtmäßig gespeicherte und für eine polizeiliche Analyseplattform zusammengeführte, personenbezogene Daten mittels einer automatisierten Anwendung zur Datenverarbeitung weiter zu verarbeiten.

III. Exekutiver Fußabdruck

Es haben keine Interessenvertreter oder beauftragte Dritte zum Inhalt des Entwurfs beigetragen.

IV. Alternativen

Alternativ kommt ein Verzicht auf entsprechende Regelungen in Betracht.

Damit blieben den Strafverfolgungsbehörden wichtige Ermittlungsinstrumente verwehrt, die in zunehmend digitalisierten Zeiten erforderlich erscheinen, um Straftaten weiterhin effektiv verfolgen zu können. Die Länder haben für den Bereich der Gefahrenabwehr teilweise bereits Ermächtigungsgrundlagen für die biometrische Fernidentifikation und für verfahrensübergreifende Analyseplattformen geschaffen oder planen dies zeitnah. Dies soll nun auch für Strafverfolgung ermöglicht werden.

V. Gesetzgebungskompetenz

Die Gesetzgebungskompetenz des Bundes folgt aus dem Kompetenztitel des Artikels 74 Absatz 1 Nummer 1 des Grundgesetzes (Gerichtsverfassung, gerichtliches Verfahren).

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

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

VII. Gesetzesfolgen

1. Rechts- und Verwaltungsvereinfachung

Keine.

2. Nachhaltigkeitsaspekte

Die beabsichtigte Einführung der neuen Ermittlungsbefugnisse trägt zur Verwirklichung von Ziel 16 „Friedliche und inklusive Gesellschaften für eine nachhaltige Entwicklung fördern, allen Menschen Zugang zur Justiz ermöglichen und leistungsfähige, rechenschaftspflichtige und inklusive Institutionen auf allen Ebenen aufbauen“ der Agenda 2030 für nachhaltige Entwicklung bei. Dieses Nachhaltigkeitsziel verlangt mit seinen Zielvorgaben 16.1, 16.2, 16.4 und 16.5, alle Formen der Gewalt und die gewaltbedingte Sterblichkeit überall deutlich zu verringern, alle Formen von Gewalt gegen Kinder zu beenden, alle Formen organisierter Kriminalität zu bekämpfen und Korruption und Bestechung erheblich zu reduzieren. Die neuen digitalen Ermittlungsbefugnisse leisten einen Beitrag zur Erreichung dieser Ziele, indem sie die Effektivität der Strafverfolgung stärken.

Der Entwurf folgt damit den Prinzipien der Deutschen Nachhaltigkeitsstrategie „(1.) Nachhaltige Entwicklung als Leitprinzip konsequent in allen Bereichen und bei allen Entscheidungen anwenden“, „(2.) Global Verantwortung wahrnehmen“ und „(5.) Sozialen Zusammenhalt in einer offenen Gesellschaft wahren und verbessern“.

3. Haushaltsausgaben ohne Erfüllungsaufwand

Es entstehen in den Haushalten des Bundes und der Gemeinden keine Haushaltsausgaben ohne Erfüllungsaufwand.

Ein Land geht davon aus, dass die Plattform zur automatisierten Datenanalyse voraussichtlich kostenneutral für die Strafverfolgung eingesetzt werden könne. Die übrigen Länder rechnen mit haushalterischen Mehrbedarfen, insbesondere wenn bei den Landespolizeien noch keine Software für die automatisierte Datenanalyse zur Gefahrenabwehr eingesetzt wird. Die Mehrbedarfe konnten jedoch nicht beziffert werden. Lediglich ein Land hat etwaige Mehrbedarfe konkretisiert, jedoch darauf hingewiesen, dass die Schätzungen nicht belastbar seien. Für eine Software zum Abgleich von biometrischen Daten wird mit jährlichen Betriebskosten zwischen 100 000 Euro und 200 000 Euro gerechnet. Für eine Recherche- und Analyseplattform werden Mehrkosten zwischen 200 000 Euro und 500 000 Euro erwartet. Potenzielle Entwicklungskosten werden im sechsstelligen Bereich veranschlagt. Für den Betrieb und die Weiterentwicklung beider Softwarelösungen wird ein Personalbedarf von 2 bis 4 Planstellen/Stellen erwartet. Auf Grundlage dieser Schätzung war eine Hochrechnung der Bedarfe sämtlicher Länder nicht möglich.

4. Erfüllungsaufwand

a) Erfüllungsaufwand für die Bürgerinnen und Bürger und für die Wirtschaft

Für die Bürgerinnen und Bürger und für die Wirtschaft entsteht kein Erfüllungsaufwand.

b) Erfüllungsaufwand der Verwaltung

Keiner.

5. Weitere Kosten

Für die Strafverfolgungsbehörden der Länder eröffnen die neuen Befugnisse die Möglichkeit, die technischen Voraussetzungen für den biometrischen Internetabgleich und die automatisierte Datenanalyse einzuführen und diese Maßnahmen anzuwenden.

Eine Schätzung der Mehrbedarfe für den biometrischen Internetabgleich war den Ländern aktuell nicht möglich, da es sich um ein gänzlich neues Ermittlungsinstrument handelt. Ein Land gab an, dass die Höhe der Kosten von einer Vielzahl derzeit nicht absehbarer Faktoren abhinge. Es wurde darauf verwiesen, dass unklar sei, wie viele Anbieter über entsprechende Software verfügten, wie deren Preisgestaltung ausfalle, wie viele Lizenzen benötigt würden und ob die Beschaffung in jedem Land separat oder gegebenenfalls in einem Länderverbund erfolgen könne. Es konnte auch nicht prognostiziert werden, wie aufwändig die Pflege und Wartung der Software ausfallen würde und – im Hinblick auf Schulungsaufwände - wie komplex die Anwendungen seien. Lediglich ein Land hat die erwarteten Aufwände beziffert und geht von jährlichen Kosten von 100 000 Euro bis 200 000 Euro aus. Für diese Schätzung wird allerdings auf Erfahrungswerte bei der Beschaffung anderer Software zurückgegriffen. Zum Teil haben die Länder auch einen nicht näher konkretisierten Personalbedarf vorgetragen.

Der Mehrbedarf für den Einsatz von Systemen zur automatisierten Datenanalyse konnte von den Ländern derzeit ebenfalls noch nicht beziffert werden. Dieser entsteht aufgrund der Notwendigkeit der Softwarebeschaffung, Weiterentwicklung und -betrieb sowie durch weitere sächliche und personelle Aufwände, wie etwa für Schulungen des mit den Maßnahmen beauftragten Personals. Bei Ländern, die heute schon im Bereich der Gefahrenabwehr Software für eine automatisierte Datenanalyse einsetzen, ist zu erwarten, dass keine neue Software angeschafft, aber vorhandene an die Vorgaben der Nutzung für die Strafverfolgung anzupassen ist.

Zwar haben die Länder teilweise ihnen bekannte Orientierungswerte für etwaige Kosten vorgetragen. So hat ein Land mitgeteilt, dass die Einführung der Plattform für die automatisierte Datenanalyse zur Gefahrenabwehr mit 25 000 000 Euroj ährlich im Haushalt veranschlagt sei. Ein weiteres Land rechnet mit jährlichen Gesamtkosten für die Polizei in vergleichbarer Höhe. Für die Mehrkosten, die mit dem erweiterten Einsatz der Analysesoftware zur Strafverfolgung verbunden sind, sind die Kosten für die Nutzung der Software zur Gefahrenabwehr jedoch unergiebig. Ein weiteres Land geht jedenfalls davon aus, dass die repressive Nutzung der Analysesoftware weitgehend kostenneutral erfolgen könne. Ein Land hat jährliche Betriebskosten zwischen 200 000 Euro bis 500 000 Euro geschätzt sowie ein Personalbedarf für Betrieb und Weiterentwicklung von 2 bis 4 Vollzeitäquivalenten für den biometrischen Internetabgleich und die automatisierte Datenanalyse. Aus diesen Schätzungen ist eine Hochrechnung der Bedarfe der übrigen Länder nicht möglich.

Auf der anderen Seite ist von kostenrelevanten Effektivitätsgewinnen auszugehen, denn es ist zu erwarten, dass durch die Anwendung der Maßnahmen aufwendigere alternative, händische Ermittlungsmaßnahmen in konkreten Ermittlungsverfahren vermieden werden können. In welcher Höhe sich Einsparpotentiale realisieren lassen, konnte von den Ländern ebenfalls nicht belastbar geschätzt werden.

Für den Generalbundesanwalt beim Bundesgerichtshof, das Bundeskriminalamt und die Bundespolizei sind infolge der neuen strafprozessualen Befugnisse keine zusätzlichen Kosten zu erwarten. Auch hier wird davon ausgegangen, dass die repressive Nutzung von bei den Polizeibehörden des Bundes eingesetzten Systemen zur automatisierten Datenanalyse und für den biometrischen Internetabgleich kostenneutral erfolgen kann.

6. Weitere Gesetzesfolgen

Die Regelungen sind inhaltlich geschlechtsneutral und betreffen alle Menschen ungeachtet ihrer sexuellen und geschlechtlichen Identität. Im Übrigen werden die Regelungen des Entwurfs keine Auswirkungen auf Verbraucherinnen und Verbraucher haben. Demografische Auswirkungen oder Auswirkungen auf die Gleichwertigkeit der Lebensverhältnisse in Deutschland sind nicht zu erwarten.

VIII. Befristung; Evaluierung

Eine Befristung der vorgeschlagenen Gesetzesänderungen kommt nicht in Betracht. Sie betreffen den Kernbereich des Strafverfahrensrechts und sind auf Dauer angelegt. Eine Evaluierung ist nicht vorgesehen. Die mit dem Gesetz eingeführten neuen Ermächtigungsgrundlagen werden grundsätzlich einer fortlaufenden Beobachtung unterzogen.

B. Besonderer Teil

Zu Artikel 1 (Änderung der Strafprozessordnung)

Zu Nummer 1 (Inhaltsübersicht)

Es handelt sich um redaktionelle Folgeänderungen der Inhaltsübersicht zu den unter Nummer 2 dargestellten Änderungen.

Zu Nummer 2

Mit § 98d und § 98e StPO-E werden spezielle Ermächtigungsgrundlagen für den Abgleich von biometrischen Daten aus einem Strafverfahren mit im Internet öffentlich zugänglichen Daten sowie zur verfahrensübergreifenden Datenanalyse mittels automatisierter Anwendungen zur Datenverarbeitung geschaffen. Mit einer automatisierten Anwendung zur Datenverarbeitung sind höher entwickelte Datenverarbeitungsprogramme gemeint, insbesondere auch solche, denen KI-Systeme im Sinne von Artikel 3 Nummer 1 der Verordnung über künstliche Intelligenz zugrunde liegen.

Ergänzend zu den neuen Regelungen in § 98d und § 98e StPO-E gelten für Systeme zur biometrischen Fernidentifizierung und verfahrensübergreifenden Datenanalyse zum Zwecke der Strafverfolgung bereits jetzt folgende Vorgaben:

Soweit bezüglich der verwendeten IT-Produkte der Anwendungsbereich der Verordnung über künstliche Intelligenz eröffnet ist – insbesondere bei sogenannten Hochrisiko-KI-Systemen gemäß Artikel 6 Absatz 2 in Verbindung mit Anhang III Nummer 1 Buchstabe a der Verordnung über künstliche Intelligenz –, gelten die entsprechenden Vorgaben unmittelbar: Solche KI-Systeme müssen daher die in der Verordnung festgelegten, unmittelbar geltenden Anforderungen an die Qualität solcher KI-Systeme und deren Sicherstellung (zum Beispiel Data-Governance, Cybersicherheit, Grundrechte-Folgenabschätzung, Konformitätsbewertungsverfahren und Registrierung des KI-Systems) erfüllen. Ein zentraler Baustein ist das Risikomanagementsystem nach Artikel 9, das vor Inverkehrbringen und während des gesamten Lebenszyklus des KI-Systems sicherstellen soll, dass etwaige Risiken für

Grundrechte, Gesundheit oder Sicherheit – einschließlich solcher durch diskriminierende Ergebnisse – frühzeitig erkannt, minimiert und überwacht werden. Artikel 9 Absatz 2 Buchstabe c verpflichtet insbesondere zur fortlaufenden Überwachung der KI-Leistung und zum Umgang mit Abweichungen und Fehlverhalten. Darüber hinaus schreibt Artikel 10 Absatz 2 Buchstabe f vor, dass bei den für Training, Validierung und Tests verwendeten Datensätzen eine sorgfältige Prüfung auf mögliche Verzerrungen („Bias“) erfolgen muss, die sich negativ auf Grundrechte oder gesetzlich geschützte Merkmale auswirken könnten. Nach Artikel 10 Absatz 3 Satz 1 müssen die Datensätze ferner „relevant, hinreichend repräsentativ, fehlerfrei und vollständig“ sein – dies ist besonders wichtig zur Vermeidung strukturell benachteiligender Trainingsgrundlagen. Ergänzend verlangt Artikel 13 Maßnahmen zur Transparenz: Hochrisiko-KI-Systeme müssen so gestaltet sein, dass ihre Ausgaben für den Nutzer verständlich sind und dieser die Ergebnisse sachgerecht bewerten kann.

Für den Einsatz von Hochrisiko-KI-Systemen zur nachträglichen biometrischen Fernidentifizierung macht die Verordnung über künstliche Intelligenz in Artikel 26 Absatz 10 zudem einschränkende, verfahrensrechtliche und materielle Vorgaben, die ab dem 1. August 2026 gelten (Artikel 113). Danach gilt insbesondere:

– Im Falle eines Abgleichs zur gezielten Suche eines Tatverdächtigen oder verurteilten Straftäters im Rahmen der Strafverfolgung muss der Abgleich durch eine bindende, justiziell überprüfbare Entscheidung einer Justiz- oder Verwaltungsbehörde vorab oder unverzüglich, spätestens jedoch binnen 48 Stunden, genehmigt werden, es sei denn der Abgleich wird zur erstmaligen Identifizierung eines potenziellen Verdächtigen auf der Grundlage objektiver und nachprüfbarer Tatsachen, die in unmittelbarem Zusammenhang mit der Straftat stehen, verwendet.

– Jede Verwendung ist auf das für die Ermittlung einer bestimmten Straftat unbedingt erforderliche Maß zu beschränken.

– Es muss sichergestellt werden, dass die Strafverfolgungsbehörden keine Entscheidung ausschließlich auf der Grundlage der Ausgabe solcher Systeme zur nachträglichen biometrischen Fernidentifizierung treffen, aus der sich eine nachteilige Rechtsfolge für eine Person ergibt.

– Es hat eine Einsatzdokumentation in der Polizeiakte zu erfolgen.

– Die Betreiber legen den zuständigen Marktüberwachungsbehörden und den nationalen Datenschutzbehörden Jahresberichte über ihre Verwendung von Systemen zur nachträglichen biometrischen Fernidentifizierung vor.

Des Weiteren müssen Hochrisiko-KI-Systeme zur biometrischen Fernidentifizierung nach Artikel 14 Absatz 5 der Verordnung über künstliche Intelligenz so gestaltet sein, dass der Betreiber keine Maßnahmen oder Entscheidungen allein aufgrund des vom System hervorgebrachten Identifizierungsergebnisses trifft, solange diese Identifizierung nicht von mindestens zwei natürlichen Personen, die die notwendige Kompetenz, Ausbildung und Befugnis besitzen, getrennt überprüft und bestätigt wurde. Dies gilt nicht, wenn die Anwendung dieser Anforderung unverhältnismäßigen Aufwand verursachen würde.

Außerdem muss beim Einsatz solcher KI-Systeme durch Strafverfolgungsbehörden beachtet werden, dass Artikel 5 Absatz 1 Buchstabe e der Verordnung über künstliche Intelligenz das Inverkehrbringen, die Inbetriebnahme für diesen spezifischen Zweck oder die Verwendung von KI-Systemen verbietet, die Datenbanken zur Gesichtserkennung durch das ungezielte Auslesen von Gesichtsbildern aus dem Internet oder von Überwachungsaufnahmen erstellen oder erweitern. Dieses Verbot gilt nicht, sofern für das Auslesen der Daten keine KI-Systeme eingesetzt werden (vergleiche Leitlinien der Europäischen Kommission zur Auslegung von Artikel 5 der Verordnung über künstliche Intelligenz, Rn. 234).

Daneben sind die bereichsspezifischen Regelungen zum Datenschutz im Strafverfahren gemäß den §§ 474 ff. StPO und – aufgrund des Verweises in § 500 StPO – nach Teil 3 des Bundesdatenschutzgesetzes (BDSG) für Datenverarbeitungssysteme im Sinne der § 98d und § 98e StPO-E anwendbar. Dies gilt insbesondere mit Blick auf die Anforderungen an die Sicherheit der Datenverarbeitung und die Durchführung einer Datenschutz-Folgenabschätzung.

Insbesondere ist die Einbindung der oder des jeweils zuständigen Datenschutzbeauftragten bereits vor der erstmaligen Einführung von neuen automatisierten Anwendungen zur Datenverarbeitung im Sinne der § 98d und § 98e aufgrund der verpflichtenden Vorgabe zur Durchführung einer Datenschutz-Folgenabschätzung sichergestellt. Eine solche ist gemäß § 500 StPO in Verbindung mit § 67 des Bundesdatenschutzgesetzes (BDSG) vor der Verwendung neuer Technologien, die – wie in den Fällen der § 98d und § 98e – aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich eine erhebliche Gefahr für die Rechtsgüter betroffener Personen zur Folge haben, durchzuführen. Gemäß § 67 Absatz 3 BDSG haben die Verantwortlichen die zuständige Datenschutzbeauftragte oder den zuständigen Datenschutzbeauftragten an der Durchführung der Folgenabschätzung zu beteiligen.

Die Strafverfolgungsbehörden unterliegen überdies fortlaufend der umfassenden, datenschutzrechtlichen Kontrolle durch die jeweils zuständigen Beauftragten für den Datenschutz (MüKoStPO/Singelnstein, 2. Aufl. 2024, StPO § 500 Rn. 9, beck-online), die ihre sich aus dem BDSG und den jeweiligen Landesgesetzen ergebenden Befugnisse ausüben können. Hiervon ist auch die Datenverarbeitung im Rahmen von Maßnahmen nach den § 98d und § 98e StPO-E durch die Strafverfolgungsbehörden erfasst.

Im Hinblick auf KI-Systeme zur nachträglichen biometrischen Fernidentifizierung schreibt Artikel 26 Absatz 10 Unterabsatz 6 der Verordnung über künstliche Intelligenz zudem unmittelbar vor, dass die Betreiber den zuständigen nationalen Datenschutzbehörden Jahresberichte über die Verwendung von entsprechenden Systemen vorzulegen haben.

Zu § 98d (Automatisierter Abgleich mit im Internet öffentlich zugänglichen biometrischen Daten)

§ 98d StPO-E regelt den automatisierten Abgleich biometrischer Daten aus einem Strafverfahren mit biometrischen Daten aus im Internet öffentlich zugänglichen Daten.

Zu Absatz 1

Ziel des biometrischen Abgleichs kann zum einen die Erforschung des Sachverhalts sein, wie dies auch bei anderen Ermittlungsmaßnahmen (etwa nach § 100a Absatz 1 Satz 1 Nummer 3 StPO) der Fall ist. Ziel der Erforschung des Sachverhalts ist es zu ergründen, ob gegen einen bestimmten Tatverdächtigen wegen einer bestimmten Straftat ein hinreichender Tatverdacht besteht oder nicht. Zu diesem Zweck sollen in gleichem Maße be- und entlastende Umstände ermittelt werden können. Zum anderen kann die Maßnahme auch der Identifizierung oder der Bestimmung des Aufenthaltsortes eines Beschuldigten oder eines Zeugen dienen. Die Maßnahme kann über § 457 Absatz 3 StPO auch als Instrument zur Fahndung zum Zwecke der Vollstreckung eines Haftbefehls dienen.

Vorausgesetzt wird, dass bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Absatz 2 bezeichnete Straftat, begangen hat, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat oder durch eine Straftat vorbereitet hat, und die Erforschung des Sachverhalts, die Identitätsfeststellung oder die Ermittlung des Aufenthaltsortes auf andere Weise wesentlich erschwert oder aussichtslos wäre.

Die materiellen Voraussetzungen entsprechen damit weitgehend denen, die auch im Falle von Maßnahmen nach den §§ 100g Absatz 1, 100i Absatz 1, 100k Absatz 1 StPO vorliegen müssen. Die Eingriffsschwelle trägt der Grundrechtsintensität der Maßnahme Rechnung. Der biometrischen Internetabgleich greift in das durch Artikel 2 Absatz 1 i.V.m. Artikel 1 Absatz 1 GG gewährleistete allgemeine Persönlichkeitsrecht in seiner Ausprägung als Recht auf informationelle Selbstbestimmung ein. Dieser Eingriff liegt in der Erfassung der Daten, ihrem Abgleich mit anderen Daten (auch bei Nicht-Treffern) und der folgenden Verwendung der Daten (vergleiche zur automatisierten Kennzeichenkontrolle nach § 163g StPO BVerfG, Beschluss vom 18. Dezember 2018 – 1 BvR 142/15 –, BVerfGE 150, 244, 289, Rn. 43). Mit der Maßnahme geht eine nicht unerhebliche Streubreite einher, weil alle Personen von der Maßnahme betroffen sind, deren öffentlich zugängliche Referenzdaten im Internet in den Abgleich einbezogen werden. Damit wird eine signifikante Zahl von personenbezogenen Daten vieler überwiegend unbeteiligter einbezogen. Biometrische Daten sind auch besonders sensible personenbezogene Daten. Allerdings werden nur die Daten derjenigen Personen, zu denen ein Treffer vorliegt, von den Strafverfolgungsbehörden überhaupt registriert. Als das Eingriffsgewicht mindernd ist daher zu berücksichtigen, dass der Datenabgleich in Sekundenschnelle durchgeführt wird und die erfassten Daten im Nichttrefferfall sofort vollständig wieder gelöscht werden, ohne einer Person bekannt zu werden und auch keine weitere polizeiliche Tätigkeit veranlassen (vergleiche am angegebenen Ort Rn. 97).

Zusätzlich zu der vorgenannten Eingriffsschwelle ist als weitere Einschränkung die Subsidiarität der Maßnahme vorgesehen. Die Maßnahme ist nur zulässig, wenn die Erforschung des Sachverhalts, die Identitätsfeststellung oder die Ermittlung des Aufenthaltsortes auf andere Weise wesentlich erschwert oder aussichtslos wäre.

Der Schutz von Berufsgeheimnisträgern ist nach der allgemeinen Schutzvorschrift des § 160a StPO gewährleistet. Soweit das europäische Medienfreiheitsgesetz (European Media Freedom Act – EMFA) Gewährleistungen zum Schutz von Medienschaffenden enthält, sind diese von den Rechtsanwendern vorrangig zu beachten und bei der Anwendung des deutschen Rechts zu berücksichtigen

Bei den für den Abgleich herangezogenen biometrischen Daten aus dem Strafverfahren können es sich beispielsweise um Daten des Beschuldigten oder eines Zeugen handeln. Diese können mit im Internet öffentlich zugänglichen biometrischen Daten abgeglichen werden. Typischer Anwendungsfall wäre ein Lichtbild oder eine Videosequenz mit dem Gesicht eines Beschuldigten oder eines relevanten Zeugen. In Betracht kämen aber beispielsweise auch Stimmaufzeichnungen. 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 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. Es sind auch solche Daten erfasst, die nach vorheriger Registrierung, Genehmigung oder Entgeltzahlung genutzt werden können. Nicht umfasst sind hingegen 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.

Zum Zweck der Durchführung des Abgleichs nach Absatz 1 können öffentlich zugängliche Daten aus dem Internet erhoben werden. Dies erlaubt zudem die (lediglich) temporäre Speicherung der Daten, um diese als Referenz für den Abgleich zu verwenden. Diese temporäre Speicherung erfolgt ausschließlich zu dem Zweck des konkreten Ausgangsverfahrens, eine weitere Verwendung der Daten ist ausgeschlossen, sie sind nach Absatz 3 zu löschen.

Nach Absatz 1 Satz 2 ist ein Abgleich mit solchen Daten unzulässig, die zum Zeitpunkt des Abgleichs ein tatsächliches Geschehen in Echtzeit widerspiegeln. Es soll damit

ausgeschlossen werden, dass eine Echtzeitüberwachung bestimmter Bereiche stattfindet. Gemeint sind damit insbesondere Live-Streams, zum Beispiel von Veranstaltungen, in denen auch das Publikum erfasst wird, oder das Live-Video einer Webcam eines öffentlich zugänglichen Ortes. Erfasst sind auch Echtzeit-Lichtbild-Sequenzen, also beispielsweise die Bilder von Webcams, die in zeitlich kurzer Abfolge einzelne Lichtbilder ins Internet hochladen.

Zu Absatz 2

Absatz 2 regelt, dass bei jeder Maßnahme die konkret eingesetzte automatisierten Anwendung zur Datenverarbeitung, der Zeitpunkt ihres Einsatzes, die Angaben, die die Feststellung der erhobenen Daten ermöglichen, und die Organisationseinheit, die die Maßnahme durchführt, zu protokollieren sind. Damit soll eine nachträgliche Überprüfung ermöglicht werden. Die Bezeichnung der eingesetzten Software dient der Transparenz. Ungeachtet dessen ist zu beachten, dass die ausgeworfenen Treffer (nebst der Webadresse) zur Akte zu nehmen sind. Die Ermittlungsbeamten müssen eine tatsächliche morphologische Übereinstimmung überprüfen und prüfen, dass die ausgeworfenen Lichtbilder auch echt, also nicht KI-generiert sind. Erst bei einem positiven Ergebnis kann der Treffer Ausgangspunkt für weitere Ermittlungsmaßnahmen sein. Sobald die Ermittlungen offen geführt werden, können die Verteidiger Akteneinsicht nehmen und die Richtigkeit der Einschätzung durch die Ermittlungsbeamten angreifen. Im Zweifel werden spätestens für die Hauptverhandlung Sachverständigengutachten eingeholt werden müssen. Dies entspricht dem Vorgehen bei der Auswertung von Videoaufzeichnungen nach der heutigen Rechtslage.

Zu Absatz 3

Nach Absatz 3 dürfen ausschließlich Daten weiterverarbeitet werden, soweit sich auf Grundlage des Abgleichs aus ihnen ein konkreter Ermittlungsansatz für das Verfahren oder anderes Strafverfahren ergibt, wobei für die Verwendung in einem anderen Strafverfahren § 479 Absatz 2 Satz 1 StPO gilt. Die Weiterverarbeitung richtet sich im Weiteren nach den allgemeinen Regelungen zur Weiterverarbeitung nach der Strafprozessordnung. Alle anderen für die Durchführung des Abgleichs aus dem Internet erhobenen und verwendeten Daten sind unverzüglich zu löschen. Dies umfasst auch etwaige aus den erhobenen Daten gewonnenen Templates, die für einen Abgleich erstellt werden. Die Vorschrift sichert eine enge Zweckbindung der Daten. Ausgeschlossen ist daher die Erstellung einer dauerhaften Datenbank, die sämtliche aus dem Internet erhobenen Lichtbilder und/oder die zugehörigen Templates enthält, die es ermöglichen würde, einen Abgleich in anderen Verfahren ohne Neuerhebung der Daten durchführen zu können.

Die Regelung in § 98d StPO ermächtigt nicht zur Inanspruchnahme ausländischer Stellen zur Durchführung des Abgleichs. Sollte die Inanspruchnahme eines Anbieters im Ausland erforderlich werden, weil die Strafverfolgungsbehörden den Abgleich technisch nicht selbst durchführen können, handelt es sich um justizielle Rechtshilfe, die sich nach dem Gesetz über die internationale Rechtshilfe in Strafsachen (IRG) richtet. Ein solches Ersuchen unterliegt dabei den Voraussetzungen zum Datenschutz der §§ 77d ff. IRG, welche eine strenge Zweckbindung zur Datenübermittlung und -verarbeitung vorsehen. Für die Staatsanwaltschaften besteht daneben die Möglichkeit, an das Bundeskriminalamt in seiner Zentralstellenfunktion (§ 2 BKAG) heranzutreten, das wiederum im Wege der sogenannten polizeilichen Rechtshilfe an ausländische Stellen herantreten könnte. Geplant ist es, eine Befugnis im Bundeskriminalamtsgesetz vorzusehen, um dem Bundeskriminalamt in seiner Zentralstellenfunktion im Falle von Straftaten, deren Verfolgung zum Schutz der nationalen Sicherheit erforderlich ist, zu ermöglichen, an Anbieter in einem Drittstaat heranzutreten (vergleiche Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit des Bundesministeriums des Innern). Diese Stellen können nach dem Entwurf auch private Anbieter sein. Dem Bundeskriminalamt kommt gemäß § 3 BKAG eine zentrale Rolle bei der internationalen Zusammenarbeit auch für die Strafverfolgung zu. Der polizeirechtliche Rechtshilfeweg erlaubt zudem erfahrungsgemäß eine zügigere Erledigung als

der justizielle und wird auch für Maßnahmen mit vergleichbarer Zielrichtung wie internationale Fahndungen oder dem Abgleich daktyloskopischer Daten typischerweise beschritten. Jedoch können über den Weg der polizeilichen Rechtshilfe lediglich Ermittlungsansätze gewonnen werden, welche für die Verwendung als Beweismittel durch ein justizielles Rechtshilfeersuchen bestätigt werden müssen. Zur Vermeidung einer Umgehung der den justiziellen Stellen vorbehaltenen Entscheidungsbefugnisse bleibt das Bundeskriminalamt im Strafverfahren stets an die Sachleitungsbefugnis der Staatsanwaltschaft gebunden (vergleiche § 9 Absatz 1 Satz 3 BKAG). Hierdurch wird sichergestellt, dass ein polizeiliches Ersuchen im laufenden Strafverfahren nur mit Zustimmung der Staatsanwaltschaften erfolgt und die gewonnenen Erkenntnisse im Rahmen des Ermittlungsverfahrens nur nach Maßgabe der staatsanwaltschaftlichen Vorgaben verwendet werden.

Zu Absatz 4

Absatz 4 sieht vor, dass der biometrischen Internetabgleich durch die Staatsanwaltschaft anzuordnen ist. Bei Gefahr im Verzug darf die Anordnung auch durch die Ermittlungspersonen der Staatsanwaltschaft (§ 152 des Gerichtsverfassungsgesetzes) erfolgen. Die Gefährdung des Untersuchungserfolgs muss stets mit Tatsachen begründet werden, die auf den Einzelfall bezogen und in den Ermittlungsakten zu dokumentieren sind, sofern die Dringlichkeit nicht evident ist (vergleiche BVerfG, Beschluss vom 12. Februar 2007 – 2 BvR 273/06 –, Rn. 17). Im Fall der Anordnung durch Ermittlungspersonen der Staatsanwaltschaft ist die Entscheidung durch die Staatsanwaltschaft unverzüglich, spätestens aber binnen 48 Stunden, herbeizuführen. Damit wird Artikel 26 Absatz 10 der Verordnung über künstliche Intelligenz Rechnung getragen. Hiernach muss beim Einsatz von KI-Systemen zur nachträglichen biometrischen Fernidentifizierung zur gezielten Suche eines Tatverdächtigen oder verurteilten Straftäters im Rahmen der Strafverfolgung der Abgleich durch eine bindende, justiziell überprüfbare Entscheidung einer Justiz- oder Verwaltungsbehörde vorab oder unverzüglich, spätestens jedoch binnen 48 Stunden, genehmigt werden, es sei denn, er wird zur erstmaligen Identifizierung eines potenziellen Verdächtigen eingesetzt. Lehnt die Staatsanwaltschaft Maßnahmen nach § 98d StPO-E nachträglich ab, so ergibt sich unmittelbar aus Artikel 26 Absatz 10 Unterabsatz 2 der Verordnung über künstliche Intelligenz, dass die Maßnahme mit sofortiger Wirkung eingestellt und im Rahmen der Maßnahme erhobene personenbezogene Daten gelöscht werden müssen.

Zu § 98e (Automatisierte verfahrensübergreifende Datenanalyse)

Mit § 98e StPO-E wird eine Ermächtigungsgrundlage für den Einsatz verfahrensübergreifender Recherche- und Analyseplattformen zur Strafverfolgung eingeführt. Dabei werden die vom Bundesverfassungsgericht in seiner Entscheidung vom 16. Februar 2023 (1 BvR 1547/19, 1 BvR 2634/20, BVerfGE 165, 363) aufgestellten Anforderungen für den Einsatz von Systemen zur automatisierten, verfahrensübergreifenden Datenanalyse oder -Auswertung personenbezogener Daten beachtet. Die Ausführungen des Bundesverfassungsgerichts zur zweckändernden automatisierten Datenverarbeitung in vorgenannter Entscheidung sind im Wesentlichen auf das Strafverfahrensrecht übertragbar.

Das Bundesverfassungsgericht hat in dieser Entscheidung ausgeführt, dass sich das Gewicht des Eingriffs in das Grundrecht auf Informationelle Selbstbestimmung (Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 GG) durch den Einsatz einer verfahrensübergreifenden automatisierten Datenanalyse oder -auswertung und die Anforderungen an die verfassungsrechtliche Rechtfertigung zum einen aus dem Gewicht der vorausgegangenen Datenerhebungseingriffe ergebe; insoweit würden auch die Grundsätze der Zweckbindung und Zweckänderung gelten. Zum anderen habe die automatisierte Datenanalyse oder -auswertung ein Eigengewicht, weil eine derartige Verarbeitung spezifische Belastungseffekte haben könne, die über das Eingriffsgewicht der ursprünglichen Erhebung hinausgingen. Aus dem Grundsatz der Verhältnismäßigkeit ergäben sich daher weitergehende Rechtfertigungsanforderungen. Das Eingriffsgewicht werde dabei insbesondere durch Art und Umfang der verarbeitbaren Daten und die zugelassene Methode der Datenanalyse oder -

auswertung bestimmt. Das Eingriffsgewicht einer solchen Befugnis könne abhängig von Datenart und -umfang und Verarbeitungsmethode potenziell sehr hoch sein. Dies wäre der Fall, wenn die Befugnis zur automatisierten Datenanalyse oder -auswertung kaum eingegrenzt wäre, da sie die Verarbeitung unbegrenzter Datenbestände in den Datenbeständen der Polizei ermögliche und die Methoden der Analyse nicht weiter einschränke. Eine solche Befugnis wäre daher nur unter denselben verfassungsrechtlichen Anforderungen zu rechtfertigen, wie sie auch bei anderen tief in die Privatsphäre eingreifenden Überwachungsmaßnahmen gelten (vergleiche zum letzten Punkt ebenda Rn. 150 f.). Unter „tief in die Privatsphäre eingreifende Überwachungsmaßnahmen“ fällt nach der Rechtsprechung des Bundesverfassungsgerichts auch die Telekommunikationsüberwachung (vergleiche BVerfG, Beschluss vom 24. Juni 2025 – 1 BvR 180/23 –, Rn. 197; BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, Rn. 103 ff.).

Die Regelung betrifft nicht die automatisierte Auswertung von in einem führenden Verfahren erhobenen und nach den §§ 474, 477 bis 480, 487 StPO oder nach den Polizeigesetzen unabhängig von einer in Absatz 1 bezeichneten Analyseplattform aus anderen Strafverfahren oder Gefahrenabwehrvorgängen konkret zum führenden Verfahren übermittelten personenbezogenen Daten. Diese richtet sich nach den allgemeinen Vorschriften.

Zu Absatz 1

Absatz 1 regelt, dass, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine auch im Einzelfall schwerwiegende, in § 100a Absatz 2 bezeichnete schwere Straftat begangen hat, in Fällen, in denen der Versuch strafbar ist, zu begehen versucht hat oder durch eine Straftat vorbereitet hat, zur Aufklärung dieser Straftat oder zur Ermittlung des Aufenthalts einer Person, nach der für die Zwecke des Strafverfahrens gefahndet wird, in Datei- und Informationssystemen der Polizei rechtmäßig gespeicherte und für eine polizeiliche Analyseplattform zusammengeführte personenbezogene Daten mittels einer automatisierten Anwendung zur Datenverarbeitung weiterverarbeitet werden dürfen. Sind in einem Verfahren sowohl Katalogtaten als auch Nicht-Katalogtaten gegenständlich, gelten dieselben Grundsätze wie bei anderen Ermittlungsmaßnahmen, die das Vorliegen einer Katalogtat zur Voraussetzung haben (vergleiche hierzu MüKoStPO/Rückert, 2. Auflage 2023, StPO § 100a, Rn. 319).

Den Strafverfolgungsbehörden wird so ermöglicht, die Daten für die Strafverfolgung auszuwerten, die die jeweiligen Polizeibehörden der Länder und des Bundes innerhalb ihres Zuständigkeitsbereichs bereits für den Betrieb einer verfahrensübergreifenden Recherche- und Analyseplattformen zur Gefahrenabwehr zusammengeführt haben. Für die Gefahrenabwehr sehen die Landesgesetze dies teilweise jetzt schon vor (vergleiche etwa für Baden-Württemberg § 47a PolG BW, Bayern § 61a PAG BY, Berlin § 47a ASOG Bln, Hamburg § 49 PolDVG HH, Hessen § 25a HSOG, Nordrhein-Westfalen § 23 Absatz 6 PolG NRW und Rheinland-Pfalz § 65a POG RP). Diese Ermächtigungsgrundlagen ermöglichen den Polizeibehörden eine Zusammenführung der in ihren Datei- und Informationssystemen gespeicherten personenbezogenen Daten, und zwar sowohl diejenigen, die sie zur Gefahrenabwehr als auch diejenigen, die sie zur Strafverfolgung erhoben haben. Zur Vermeidung von Doppelstrukturen soll § 98e StPO-E die Möglichkeit eröffnen, die bereits zusammengeführten Daten auch zur Strafverfolgung zu nutzen. Damit wird die Einrichtung einer separaten verfahrensübergreifenden Analyseplattform und damit auch eine weitere, separate Zusammenführung dieser Daten für die Strafverfolgung entbehrlich. Die Datenbestände, die für die Strafverfolgung relevant sind, decken sich im Wesentlichen mit den Datenbeständen, die von der Polizei für die Zwecke der Gefahrenabwehr zusammengeführt werden, da bei den Polizeibehörden auch der wesentliche Teil der Daten aus der Strafverfolgung gespeichert ist (vergleiche MüKoStPO/Singelnstein, 2. Auflage 2024, StPO, Vorbemerkung zu § 483 Rn. 4, beck-online) und für die Zwecke der Strafverfolgung auch die Daten aus der Gefahrenabwehr relevant sind (vergleiche § 98c StPO).

Mit dem in Absatz 1 verwendeten Begriff „Datei- und Informationssystemen der Polizei“ sind die Systeme der jeweiligen Landespolizeien bzw. der Polizeibehörden des Bundes gemeint, in denen für die Strafverfolgung und Gefahrenabwehr personenbezogene Daten rechtmäßig gespeichert werden. In Absatz 2 wird näher definiert, welche Datenbestände hiervon zur Strafverfolgung in eine Datenweiterverarbeitung einbezogen werden dürfen.

Die Zusammenführung bedeutet, dass die Daten einheitlich durchsuchbar gemacht werden. Die bisher aufwendige Suche in einzelnen Datenbanken, die ein mehrfaches manuelles Anstoßen eines Suchvorgangs erfordert, wird durch die Zusammenführung überwunden. Diese kann beispielsweise durch vorherige Spiegelung der Daten auf der Analyseplattform erfolgen. Die für die speichernde Stelle geltenden gesetzlichen Vorgaben für die Verarbeitung personenbezogener Daten und die Rechte der Betroffenen einschließlich der geltenden Übermittlungsvorschriften und Verwendungsregelungen gelten dabei fort. Dies betrifft insbesondere auch die Speicher- und Löschfristen, die Kennzeichnungspflichten und etwaige Vorgaben zu Rollen- und Rechtekonzepten. Diese gelten in derselben Weise für die Daten nach deren Zusammenführung und sind daher zwingend technisch in das System zu implementieren, soweit hierzu in der jeweiligen polizeirechtlichen Ermächtigungsgrundlage keine besonderen Regelungen getroffen worden sind (vergleiche etwa die Regelung in § 25a Absatz 2 HSOG zum besonderen Rollen- und Rechtekonzept und Konzept der Kategorisierung und Kennzeichnung personenbezogener Daten). Insbesondere zieht das Zusammenführen von Daten keine Verlängerung der Speicherfristen nach sich. Die Speicherfristen und Löschpflichten aus dem jeweiligen Quellsystem gelten vielmehr fort (vergleiche etwa Drucksache des Bayerischen Landtags 19/1557, Seite 26).

Durch die Verwendung des Begriffs „Dateisystem“ werden elektronische Akten ausgeschlossen, da elektronische Akten und elektronische Aktenkopien gemäß § 496 Absatz 3 StPO keine Dateisysteme im Sinne der §§ 483 ff. StPO sind (Tillich in: Löwe-Rosenberg, StPO, 27. Auflage 2024, Vorbemerkungen zu §§ 483 ff., Rn. 15). Die bei Staatsanwaltschaften geführten elektronischen Akten gehören damit nicht zu den Daten, die für eine solche Analyseplattform zusammengeführt werden können. Der maschinelle Abgleich personenbezogener Daten mit elektronischen Akten oder elektronischen Aktenkopien richtet sich nach § 498 Absatz 2 StPO. Ungeachtet dessen können Daten, die aus den in Absatz 2 genannten Datenbeständen stammen und auch Gegenstand der elektronischen Strafverfahrensakte geworden sind, weiterhin unter den in § 98e StPO aufgestellten Voraussetzungen in die Analyse mit einbezogen werden.

Es dürfen nur solche Daten einbezogen werden, die rechtmäßig gespeichert sind. Sie müssen also nach den einschlägigen gefahrenabwehrrechtlichen oder strafprozessualen Regelungen über die Erhebung von Daten rechtmäßig erhoben worden und im Einklang mit den anwendbaren polizeirechtlichen (also beispielsweise §§ 22 ff. PolG NRW, §§ 55 ff. PAG BY, §§ 12 ff. BKAG) oder strafprozessualen (§§ 483 ff. StPO) datenschutzrechtlichen Vorgaben abgespeichert sein.

Um die durch § 98e StPO-E eröffnete Möglichkeit zu nutzen, müssten in den entsprechenden Landespolizeigesetzen und in den die Polizeibehörden des Bundes betreffenden Gesetzen spiegelbildlich Regelungen geschaffen werden, die die Nutzung ihrer zum Zwecke der Gefahrenabwehr für Analyseplattformen zusammengeführten Daten für Zwecke der Strafverfolgung nach Maßgabe von § 98e StPO-E ermöglichen.

Zu Absatz 2

Nach Absatz 2 Satz 1 dürfen bei der Weiterverarbeitung Vorgangsdaten, Falldaten, Daten aus den polizeilichen Informationssystemen und aus dem polizeilichen Informationsaustausch einbezogen werden.

Vorgangsdaten sind sämtliche Daten, die im Zusammenhang mit einer polizeilichen Tätigkeit bei einem bestimmten Einsatzanlass zu Personen und Sachen im polizeilichen

Vorgangsbearbeitungssystem erfasst werden. Aufgenommen werden insbesondere Anzeigen, Ermittlungsberichte und Vermerke, die nicht nur Daten zu Verdächtigen, Beschuldigten oder sonstigen Anlasspersonen enthalten, sondern beispielsweise auch zu Personen, die Anzeige erstatten, Hinweise geben oder Zeuginnen oder Zeugen sind. Vorgangsdaten werden in Vorgangsbearbeitungssystemen erfasst und mittels Vorgangsverwaltungssystemen verwaltet (vergleiche Gesetzesbegründung zu § 49 PolDVG HH, Bürgerschaft der Freien und Hansestadt Hamburg, Drucksache 22/16042, Seite 29 f.). Da die Daten aus der Vorgangsverwaltung auch Unbeteiligte betreffen, führt die Einbeziehung dieser Daten zu einer Erhöhung des Eingriffsgewichts (vergleiche auch Gesetzesbegründung zu § 47a PolG BW, Drucksache des Baden-Württembergischen Landtags 17/9478). Bereits heute sind Daten aus den Vorgangsbearbeitungs- und verwaltungssystemen im Wege eines einfachen Datenabgleichs über die Suchmaske des jeweiligen Systems mittels Indexsuche durchsuchbar.

Falldaten ergeben sich aus sogenannten Fallbearbeitungssystemen. Dabei handelt es sich um automatisierte Verfahren zur strukturierten Bearbeitung von umfangreichen Ermittlungsverfahren. Ein gängiges, aktuell von Landespolizeien zur Fallbearbeitung eingesetztes Programm ist die Software „Crime“ (vergleiche etwa Gesetzesbegründung zu § 49 PolDVG HH, Bürgerschaft der Freien und Hansestadt Hamburg, Drucksache 22/16042, Seite 30; Gesetzesbegründung zu § 47 PolG-E BW, Drucksache des Baden-Württembergischen Landtags 17/9478).

Polizeiliche Informationssysteme enthalten personenbezogene Informationen, die sowohl zum Zweck der Verhütung von Straftaten als auch zum Zweck der Strafverfolgung und -vollstreckung gespeichert werden. Das gängige von den Ländern eingesetzte polizeiliche Informationssystem heißt „POLAS“, „POLIS“ oder „INPOL-Land“ (vergleiche etwa Gesetzesbegründung zu § 49 PolDVG HH, Bürgerschaft der Freien und Hansestadt Hamburg, Drucksache 22/16042, Seite 30; vergleiche auch Gesetzesbegründung zu § 47 PolG-E BW, Drucksache des baden-württembergischen Landtags 17/9478; Gesetzesbegründung zu § 25a HSOG, Drucksache des Hessischen Landtags 20/11235, Seite 12 f.). Das Informationssystem des Bundeskriminalamts findet seine Grundlage in § 13 BKAG („INPOL-Neu“); es ist Hauptbestandteil des polizeilichen Informationsverbunds gemäß § 29 BKAG. Die von den Ländern eingesetzten polizeilichen Informationssysteme sind an „INPOL-Neu“ angeschlossen. Die polizeilichen Informationssysteme bestehen aus unterschiedlichen Datengruppen. Hierzu gehören insbesondere Kriminalaktennachweise, Personenfahndungen, Sachfahndungen, Haftdateien, Erkennungsdienst und DNA-Analyse-Dateien.

Daten aus dem polizeilichen Informationsaustausch sind zwischen den Polizeien des Bundes und der Länder ausgetauschte polizeiliche Informationen mit hoher Relevanz insbesondere zu überregionalen Straftätern, zu serienmäßig begangenen Straftaten oder zu akuten Gefahrensachverhalten. Derzeit wird hierfür überwiegend das bundesweite, webbasierte Fernschreibsystem EPOST 810 genutzt (vergleiche Gesetzesbegründung zu § 25a HSOG, Drucksache des Hessischen Landtags 20/11235, S. 14; Gesetzesbegründung zu § 49 PolDVG HH, Bürgerschaft der Freien und Hansestadt Hamburg, Drucksache 22/16042, Seite 30).

Absatz 2 Satz 2 regelt, dass die aufgrund von Maßnahmen nach den §§ 100a, 100f, 100g, 100k Absatz 1, Absatz 2, 100i StPO in anderen Strafverfahren oder entsprechenden Maßnahmen nach anderen Gesetzen gewonnenen sowie die aus Asservaten stammenden personenbezogenen Daten nur dann in die automatisierte Weiterverarbeitung einbezogen werden können, soweit dies erforderlich ist. Dies betrifft zum einen Verkehrsdaten, wie etwa Verbindungsdaten einschließlich Standortdaten, die durch Telekommunikationsüberwachungsmaßnahmen gemäß § 100a StPO, durch Funkzellenabfragen gemäß § 100g StPO oder unter Einsatz eines IMSI-Catchers auf der Grundlage des § 100i Absatz 1 Nummer 2 StPO oder im präventiven Bereich nach den entsprechenden Polizeigesetzen der Länder oder des Bundes erhoben werden können. Erfasst sind aber auch Inhaltsdaten aus Telefonüberwachungsmaßnahmen. Mit den aus Asservaten stammenden personenbezogenen

Daten sind Daten gemeint, die aus beschlagnahmten oder sichergestellten Datenträgern stammen. Nicht betroffen sind beispielsweise Anzeigen, Ermittlungsberichte und Vermerke, die sich auf solche Daten beziehen oder eine Zusammenfassung einer Auswertung enthalten und aufgrund dessen bereits Eingang in Vorgangsdaten oder Falldaten gefunden haben.

Diese Daten dürfen in die Analyse ergänzend einbezogen werden, soweit dies erforderlich ist. Dies ist der Fall, wenn die Daten für die Zwecke des konkreten Verfahrens benötigt werden, und wenn bereits vor Kenntnis vom Inhalt der Daten tatsächliche Anhaltspunkte dafür vorliegen, dass die einzubeziehenden Daten in Verbindung zum konkreten Suchanlass stehen könnten (vergleiche zu Asservaten die Gesetzesbegründung zu § 47 PolG-E BW, Drucksache des Baden-Württembergischen Landtags 17/9478, Seite 27). Damit soll vermieden werden, dass bei jeder Suche von vorne herein sämtliche, zu allen Verfahren bei der Polizei gespeicherten, oben benannten Datenbestände nach Anhaltspunkten für weitere Ermittlungen durchsucht werden. Es soll sichergestellt sein, dass im Vorfeld der Analyse eine sich an kriminalistischen Kriterien orientierende Vorauswahl an Datenbeständen getroffen wird, die einbezogen werden sollen. Eine solche Vorauswahl kann beispielsweise auf Basis von persönlichen oder sachlichen Bezügen der anderen Verfahren zum führenden Ermittlungsverfahren getroffen werden. Ein sachlicher Bezug kann auch in der Zugehörigkeit der Verfahren zu einem bestimmten Deliktsbereich bestehen.

Schließlich sieht Absatz 2 Satz 3 vor, dass die aufgrund der sehr eingriffsintensiven Maßnahmen einer Online-Durchsuchung oder einer Wohnraumüberwachung nach § 100b und § 100c StPO in anderen Strafverfahren oder entsprechenden gefahrenabwehrrechtlichen Maßnahmen erlangten, personenbezogenen Daten in eine automatisierte Datenverarbeitung nach Absatz 1 nicht einbezogen werden dürfen. Hintergrund ist die regelmäßige besondere Sensibilität der bei diesen Maßnahmen gewonnenen Daten. In den gefahrenabwehrrechtlichen Regelungen der Länder finden sich teilweise entsprechende Vorgaben (vergleiche § 25a Absatz 3 Nummer 2b HSOG und § 49 Absatz 2 Satz 7 PolDVG Hamburg).

Zu Absatz 3

Mit der Beschränkung auf Datei- und Informationssysteme der Polizei in Absatz 1 ist eine umfassende Einbeziehung externer öffentlicher Quellen (Internet) sowie sonstiger, nicht von der Polizei betriebener Datenbanken (Beispielsweise: Melderegister, Personalausweisregister, Ausländerzentralregister) für die Strafverfolgung nicht vorgesehen. Absatz 3 stellt daher klar, dass eine direkte Anbindung der Analyseplattform an sonstige nicht-polizeiliche Register und an Internetdienste ausgeschlossen ist. Datensätze aus gezielten, auch automatisierten Abfragen [vergleiche etwa § 34 Absatz 2 Bundesmeldegesetz (BMG) in Verbindung mit § 34a BMG oder § 36 Absatz 2 Straßenverkehrsgesetz] in sonstigen staatlichen, nicht-polizeilichen Registern und einzelne als Ergebnis einer zielgerichteten Recherche gesondert gespeicherte Datensätze aus Internetquellen können in die Weiterverarbeitung aber einbezogen werden. Bereits in den Datenbanken der Polizei vorhandene, im Einzelfall in anderen Verfahren oder Vorgängen abgerufene Daten können ebenfalls einbezogen werden.

Zu Absatz 4

Absatz 4 enthält eine abschließende Beschreibung, wie die automatisierte Anwendung zur Datenverarbeitung im Rahmen der Datenweiterverarbeitung vorgehen kann.

Technisch erfolgt vom Grundsatz her ein Abgleich von (personenbezogenen) Daten aus den angebundenen Quellsystemen (vergleiche Drucksache des Bayerischen Landtags 19/1557, Seite 25). Im Rahmen der Weiterverarbeitung können hiervon ausgehend nach Absatz 4 Satz 1 Nummer 1 datei- und informationssystemübergreifend Beziehungen oder Zusammenhänge zwischen Verfahren, Vorgängen, Personen, Personengruppierungen,

Institutionen, Organisationen, Orten, Objekten und Sachen identifiziert und hergestellt, sowohl qualitativ als auch quantitativ klassifiziert, strukturell analysiert und visualisiert werden. Dabei können für die Erreichung des Zwecks der Weiterverarbeitung unbedeutende Informationen und Erkenntnisse ausgeschlossen und die eingehenden Erkenntnisse zu bekannten Sachverhalten zugeordnet werden (Absatz 4 Satz 1 Nummern 2 und 3). Hierfür muss das System technisch die Möglichkeit haben, Suchkriterien zu gewichten (Absatz 4 Satz 1 Nummer 4), insbesondere nach Sachnähe, Aktualität und Erheblichkeit der Verknüpfung mit anderen Informationen bezogen auf den Zweck der Weiterverarbeitung nach Absatz 1.

Die Methodik der automatisierten Anwendung zur Datenverarbeitung hat sich dabei darauf zu beschränken, in Datei- und Informationssystemen der Polizei gespeicherte Daten aufzubereiten und bereitzustellen. Das Ergebnis der Weiterverarbeitung muss immer erkennen lassen, welche in den Datei- und Informationssystemen der Polizei gespeicherten Daten ihm aus welchem Grund zugrunde liegen, sodass von den ermittelnden Beamten eigene Bewertungen und Entscheidungen getroffen werden können. Dies stellen die Sätze 2 und 4 klar. Die Anwendung darf nach Satz 3 nur aufgrund eines konkreten Anlasses erfolgen und anhand von Suchkriterien, die sich aus dem konkreten Sachverhalt ergeben. Offene Suchen nach Zusammenhängen „ins Blaue hinein“ sind damit ausgeschlossen. Der Einsatz der Analyseplattform dient damit allein dazu, den Rechercheaufwand zu reduzieren, damit der zuständige Sachbearbeiter sich vorwiegend auf die eigentliche Analyse konzentrieren kann. Sie soll es dem Ermittlungsbeamten ermöglichen, mittels einer einheitlichen Software die rechtmäßig in den Datei- und Informationssystemen der Polizei gespeicherten Daten der Gefahrenabwehr und Strafverfolgung umfassend, schnell und effizient durch eine Vielzahl zeitgleich ausgeführter Datenabgleiche auf Querverbindungen zum eigenen Strafverfahren zu untersuchen, deren Bedeutung aber sodann der Ermittlungsbeamte selbst zu bewerten hat. Prognostische Scoring-Funktionen, die Personen anhand von Risikobewertungen kategorisieren, sind mit diesen Methodenvorgaben ausgeschlossen, zumal solche Funktionen für die Strafverfolgung ohnehin keine Relevanz haben. Ebenfalls ausgeschlossen sind die Erzeugung synthetischer Ermittlungsansätze oder hypothetischer Tatszenarien.

Diese einschränkenden Vorgaben führen zu einer Reduktion des Eingriffsgewichts in die betroffenen Grundrechte. Denn das Eingriffsgewicht wird nach den Ausführungen des Bundesverfassungsgerichts in seiner Entscheidung vom 16. Februar 2023 (1 BvR 1547/19, 1 BvR 2634/20 – dort Rn. 91 ff.) umso geringer, je mehr der Vorgang der automatisierten Datenanalyse oder -auswertung methodisch einem einfachen Datenabgleich angenähert ist. Die Komplexität des suchenden Vergleichs könne sich zwar durch eine höhere Zahl an Abgleichschritten und Verknüpfungen erhöhen. Das Eingriffsgewicht sei aber insbesondere dann umso höher, je offener die Methode des Suchvorgangs gestaltet sei und je weniger die automatisierte Datenanalyse oder -auswertung durch – auch mit Erkenntnissen und Annahmen zu dem konkreten Sachverhalt gespeiste – polizeiliche Suchmuster gesteuert werde. Eingriffserhöhend wirke es überdies, wenn das Ergebnis maschinelle Sachverhaltsbewertungen enthalte, die also über die bloße Anzeige von Übereinstimmungen zwischen dem Suchkriterium und den durchsuchten Daten hinausgingen. Offene Suchen werden mit den Methodenvorgaben ausgeschlossen. Maschinelle Sachverhaltsbewertungen können nur innerhalb der in Absatz 4 vorgesehenen Grenzen stattfinden.

Dabei wird mit Blick auf die vom Bundesverfassungsgericht geäußerte Besorgnis, dass eine Analysesoftware die polizeiliche Arbeit möglicherweise so verändert, dass der Faktor Mensch in den Hintergrund trete und dass die Software von Menschen getroffene Entscheidungen sogar ersetzen könnte, mit den Vorgaben in den Sätzen 2 bis 4 sichergestellt, dass der Mensch am Anfang und am Ende des Entscheidungsprozesses steht. Die Analyseplattform soll die Arbeitsweise der Strafverfolgungsbehörden nicht entscheidend verändern, sondern lediglich dabei unterstützen, Informationen aus verschiedenen Quellen zusammenzutragen und sie zu bewerten. Damit ist sichergestellt, dass eine Analysesoftware ein reines Hilfsinstrument bleibt. Satz 4 stellt ausdrücklich klar, dass eine ausschließlich auf der Maßnahme nach Absatz 1 beruhende automatisierte Entscheidungsfindung, die

unmittelbar eine nachteilige Rechtsfolge für die betroffene Person hat oder diese erheblich beeinträchtigt, unzulässig ist.

Der Einsatz künstlicher Intelligenz und der Einsatz von Sprachmodellen ist in den Grenzen der von der Ermächtigungsgrundlage vorgegebenen Auswertemethoden möglich und kann damit für sämtliche in Absatz 4 beschriebenen Anwendungsfälle genutzt werden. Insbesondere kann der Einsatz künstlicher Intelligenz dazu dienen, die technischen Möglichkeiten zu verbessern und im Rahmen des Datenabgleichs Ähnlichkeiten in Sachverhalten zu erkennen (beispielsweise beim modus operandi oder bei Organisationsstrukturen). Viele Systeme künstlicher Intelligenz nutzen statistische Modelle und Wahrscheinlichkeiten. Absatz 4 Satz 1 Nummer 5 sieht daher auch vor, dass gespeicherte Daten statistisch ausgewertet werden können.

Um zu vermeiden, dass sich mit dem Einsatz automatisierter Analysesysteme in der Polizeiarbeit spezifische Diskriminierungsrisiken verwirklichen, ordnet Satz 5 zudem ausdrücklich an, dass technisch und organisatorisch sicherzustellen ist, dass diskriminierende Algorithmen weder herausgebildet noch verwendet werden.

Zu Absatz 5

Zur Gewährleistung von Kontrolle und Transparenz regelt Absatz 5 Satz 1, dass der Einsatz der automatisierten Anwendung zur Datenverarbeitung unter Darlegung der Voraussetzungen nach Absatz 1, bei Einbeziehung von Daten nach Absatz 2 Satz 2 unter Darlegung auch der hierfür geltenden Voraussetzungen, zu begründen ist. Dies kann etwa dadurch erfolgen, dass das System eine entsprechende Eingabemaske vorsieht, in der die im konkreten Verfahren in Betracht kommenden Straftaten und die den Verdacht begründenden Tatsachen einzugeben oder auszuwählen sind, sowie kurz begründet werden kann, aus welchen Gründen die in Absatz 2 Satz 2 genannten Datenbestände einbezogen werden sollen.

Zudem sieht Absatz 5 Satz 2 vor, dass die Einsätze zu protokollieren sind. Damit soll nachvollziehbar bleiben, welche Datenbestände wann und warum einbezogen worden sind. Die Protokollierung kann beispielsweise dadurch erfolgen, dass die Analysesoftware technisch sicherstellt, dass jeder Anwendungsvorgang automatisiert in seinen wesentlichen Schritten fortlaufend gespeichert wird. Soweit sich besondere, hierüber hinausgehende Protokollierungspflichten aus den polizeirechtlichen Regelungen ergeben, greifen diese. Die Begründungspflicht und die Protokollierung bei der Nutzung des Analysetools sichert die aufsichtliche Kontrollmöglichkeit durch den zuständigen Datenschutzbeauftragten und ist gleichzeitig Voraussetzung für die Gewährleistung effektiven Rechtsschutzes (vergleiche auch Gesetzesbegründung zu § 25a HSOG, Drucksache des Hessischen Landtags 20/11235, Seite 17). Auch die gefahrenabwehrrechtlichen Ermächtigungsgrundlagen für den Einsatz derartiger Analysesysteme sehen Begründungs- und Dokumentationspflichten vor (vergleiche etwa § 25a Absatz 4 HSOG, § 49 Absatz PolDVG HH, § 65a Absatz 7 POG RP).

Zu Absatz 6

Absatz 6 stellt für die in Absatz 2 genannten Daten insgesamt klar, dass auch das für die speichernde Stelle geltende Recht über die Verarbeitung personenbezogener Daten und die Rechte der Betroffenen einschließlich der anwendbaren Übermittlungsvorschriften und Verwendungsregelungen zu beachten und dass dessen Einhaltung technisch und organisatorisch sicherzustellen ist.

Ob für die Verarbeitung personenbezogener Daten und die Rechte der Betroffenen seitens der jeweiligen Landespolizei oder Polizeibehörde des Bundes die jeweils einschlägigen polizeirechtlichen oder strafprozessualen Vorschriften nach den §§ 483 ff. StPO zu beachten sind, richtet sich bei Daten aus der Strafverfolgung danach, ob die einbezogenen Daten in den Systemen der jeweiligen Polizei in sogenannten Mischdateisystemen zusammen mit

Daten aus der Gefahrenabwehr nach § 483 Absatz 3 StPO oder ob sie in Dateisystemen gespeichert sind, in denen ausschließlich Daten aus der Strafverfolgung liegen. Für sogenannte Mischdateisysteme ordnet § 483 Absatz 3 StPO insgesamt die Geltung polizeirechtlicher Vorschriften an. Für polizeiliche Informationssysteme gelten unter Berücksichtigung von § 483 Absatz 1 Satz 2 und Satz 3 StPO die polizeirechtlichen Vorschriften, soweit Daten aus der Gefahrenabwehr betroffen sind, und die §§ 483 ff. StPO bei Daten aus der Strafverfolgung. Bei sonstigen Dateisystemen, in denen ausschließlich Daten aus der Strafverfolgung gespeichert sind, gelten die §§ 483 ff. StPO. Im Hinblick auf die in polizeilichen Dateisystemen gespeicherten Daten aus der Gefahrenabwehr gelten immer die jeweils einschlägigen polizeirechtlichen Vorschriften. Die Zusammenführung der Daten und der Zugriff hierauf über die Analyseplattform führt nicht zu einer rechtlichen Loslösung von den hiernach für die speichernde Stelle geltenden gesetzlichen Vorgaben. Deren Einhaltung ist daher auch bei dem Betrieb der Analyseplattform zwingend technisch und organisatorisch sicherzustellen. Die Zusammenführung führt – wenn hierzu eine Spiegelung von Daten erfolgt – bezüglich der gespiegelten Daten auch nicht zu einem Mischsystem gemäß § 483 Absatz 3 StPO.

Dies bedeutet beispielsweise, dass für Daten aus der Strafverfolgung, die in nur für Daten aus der Strafverfolgung bestimmten Dateisystemen oder in Informationssystemen der Polizei gespeichert sind, auch im Rahmen der Verarbeitung der Daten in der Analyseplattform weiterhin § 487 Absatz 1 StPO gilt, dessen Vorgaben technisch zu implementieren sind. Nach § 487 Absatz 1 Satz 1 StPO dürfen die nach den §§ 483 bis 485 StPO gespeicherten Daten nur übermittelt werden, soweit dies für Zwecke eines bestimmten Strafverfahrens, für Zwecke eines Gnadenverfahrens, des Vollzugs von freiheitsentziehenden Maßnahmen oder der internationalen Rechtshilfe in Strafsachen erforderlich ist. Nach § 487 Absatz 1 Satz 2 StPO gelten § 479 Absatz 1 und Absatz 2 StPO entsprechend. Aus der entsprechenden Anwendung von § 479 Absatz 1 StPO ergibt sich, dass eine Verwendung von personenbezogenen Daten für ein anderes Strafverfahren ausgeschlossen ist, wenn dieser Verwendung Zwecke des Strafverfahrens, aus dem die Daten stammen, auch die Gefährdung des Untersuchungszwecks in einem anderen Strafverfahren, oder besondere bundesgesetzliche oder landesgesetzliche Verwendungsregelungen entgegenstehen.

Zu den besonderen bundesgesetzlichen, strafprozessualen Verwendungsregelungen zählen zum Beispiel die Verwendungsbestimmungen für (vergleiche MüKoStPO/Singelnstein, 2. Auflage 2024, StPO § 479 Rn. 17, beck-online):

– Bild-Ton-Aufzeichnungen von Zeugenvernehmungen (§ 58a Absatz 2, § 247a Absatz 1 Satz 5 StPO), für die eine strenge Zweckbindung gilt,

– den Zeugenschutz bei Angaben des Zeugen zur Person (§ 68 Absatz 5 StPO),

– Daten, die unter Verletzung des Kernbereichs privater Lebensgestaltung erlangt wurden (§ 100d Absatz 2 Satz 1 StPO), die ganz allgemein und auch ohne gesonderte Regelung unter keinen Umständen übermittelt werden dürfen,

– personenbezogene Daten Dritter, die beim Einsatz eines IMSI-Catchers erhoben werden (§ 100i Absatz 2 Satz 2 StPO),

– Daten aus verdeckten Maßnahmen, deren Löschung für Zwecke des Rechtsschutzes zurückgestellt wurde (§ 101 Absatz 8 Satz 3 StPO),

– Daten aus Kontrollen (§ 163d Absatz 1 Satz 3 StPO),

– Vorgaben für amtlich verwahrte Schriftstücke (§ 96 StPO),

– bestimmte Daten im Rahmen der Rasterfahndung (§ 98a Absatz 3 Satz 2 StPO).

Als weitere, besonders bedeutsame bundesgesetzliche, strafprozessuale Verwendungsregel ist die Regelung zum hypothetischen Ersatzeingriff nach § 161 Absatz 3 StPO für die Verwendung von personenbezogenen Daten aus der Gefahrenabwehr, die mit besonders eingriffsintensiven Ermittlungsmaßnahmen erhoben wurden, zu nennen (vergleiche MüKoStPO/Singelnstein, 2. Auflage 2024, StPO § 479 Rn. 17).

Auch weitere sich etwa aus den §§ 97, 100g Absatz 4, 108 Absatz 2 und 3, 136a, 148 StPO ergebende strafprozessuale Schutzvorschriften zählen hierzu (vergleiche BeckOK StPO/Gerhold, 55. Ed. 1.4.2025, StPO § 98c Rn. 13, beck-online; MüKoStPO/Singelnstein, 2. Auflage 2024, StPO § 479 Rn. 19, beck-online).

Zu nennen ist auch der Schutz von Berufsgeheimnisträgern nach § 160a StPO. Demgemäß ändert sich auch das Niveau, mit dem Berufsgeheimnisträger geschützt sind, nicht. Soweit das europäische Medienfreiheitsgesetz (European Media Freedom Act – EMFA) Gewährleistungen zum Schutz von Medienschaffenden enthält, sind diese von den Rechtsanwendern vorrangig zu beachten und bei der Anwendung des deutschen Rechts zu berücksichtigen.

Schließlich gilt über den Verweis in § 487 Absatz 1 Satz 2 StPO auch § 479 Absatz 2 StPO. § 479 Absatz 2 StPO regelt die Grundsätze des sogenannten hypothetischen Ersatzeingriffs für die Verwendung von personenbezogenen Daten, die in anderen Strafverfahren mit besonders eingriffsintensiven Ermittlungsmaßnahmen erhoben wurden.

Für Daten aus der Gefahrenabwehr oder Daten aus der Strafverfolgung, die in Mischdateisystemen nach § 483 Absatz 3 StPO gespeichert sind, gelten weiterhin die jeweiligen polizeirechtlichen Übermittlungsvorschriften und Verwendungsregelungen, die insbesondere auch Regelungen zum sogenannten hypothetischen Ersatzeingriff enthalten. Hierzu zählen beispielsweise § 12 und § 22 Absatz 2 BKAG.

Mit Absatz 6 Satz 1 wird aber auch klargestellt, dass die sich aus den §§ 483 ff. StPO oder den jeweiligen polizeirechtlichen Vorschriften ergebenden Vorgaben zu den Speicher- und Löschfristen, den Kennzeichnungspflichten und etwaigen Rollen- und Rechtekonzepten, in derselben Weise für die Daten nach deren Zusammenführung zum Zwecke des Betriebs der Analyseplattform fortgelten. Insbesondere zieht das Zusammenführen der Daten keine Verlängerung der Speicherfristen in den Quellsystemen nach sich. Vielmehr kommt es zu einem automatischen Durchgreifen der Speicherfristen und Löschpflichten aus den jeweiligen Quellsystemen. Für Daten aus der Strafverfolgung, die nicht in Mischdateisystemen nach § 483 Absatz 3 StPO gespeichert sind, gelten daher auch die Vorgaben aus der jeweiligen Errichtungsanordnung nach § 490 StPO fort, insbesondere die zu den Prüffristen und zur Speicherdauer. Soweit für Daten polizeirechtliche Vorschriften gelten, können sich die Vorgaben zu den Speicher- und Löschfristen, den Kennzeichnungspflichten und etwaigen Rollen- und Rechtekonzepten aus entsprechenden landesrechtlichen Vorschriften oder Vorschriften auf Bundesebene ergeben. Enthält die jeweilige, polizeirechtliche Ermächtigungsgrundlage für den Betrieb der Analyseplattform hierzu besondere Regelungen, greifen diese und sind in entsprechender Form für den Einsatz der Analyseplattform zum Zwecke der Strafverfolgung umzusetzen. Dies gilt insbesondere für etwaige besondere Regelungen in den polizeirechtlichen Ermächtigungsgrundlagen zu Rollen- und Rechtekonzepten und besonderen Konzepten der Kategorisierung und Kennzeichnung personenbezogener Daten, wie etwa in § 25a Absatz 2 HSOG, § 49 Absatz 3 PolDVG HH oder § 65a Absätze 4 bis 6 POG RP. Die polizeirechtlichen Regelungen zur Entwicklung, Überprüfung, Änderung oder zum Trainieren von IT-Produkten einschließlich selbstlernender Systeme sind ebenfalls entsprechend anwendbar.

Nach Absatz 6 Satz 2 ist die Einhaltung dieser Verwendungsregelungen, insbesondere der § 161 Absatz 3 Satz 1 und 2 sowie § 479 Absatz 2 Satz 1 StPO technisch und organisatorisch sicherzustellen. Dies kann etwa über die Kennzeichnung der Daten erfolgen und dadurch, dass diese nur bei Vorliegen der Voraussetzungen der entsprechenden

Übermittlungs- und Verwendungsregelungen für eine automatisierte Einbeziehung in die Datenanalyse technisch zur Verfügung stehen.

Zu Nummer 3

Zu Buchstabe a

§ 101 StPO trifft Verfahrensregelungen für verdeckte Maßnahmen. § 98d wird in die Aufzählung der verdeckten Maßnahmen aufgenommen, sodass die Verfahrensregelungen unmittelbare Anwendung finden. Dies umfasst insbesondere Regelungen zu Kennzeichnungs- (§ 101 Absatz 3 StPO) und Benachrichtigungspflichten (§ 101 Absatz 4 bis 7 StPO; vergleiche 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. Das Löschgebot besteht beispielsweise dann, wenn sich nach einem Treffer der Aufenthalt oder die vermutete Identität des Betroffenen bestätigen lässt, etwa durch den Abgleich mit einer anderen Quelle (beispielsweise Abruf seines Lichtbilds aus dem Personalausweisregister), und den erhobenen Daten nicht zufälligerweise sonstige Beweisbedeutung für das konkrete Strafverfahren zukommt. Die Löschvorschrift stellt so sicher, dass Bild-, Audio- und Videomaterial oder andere Dateien mit biometrischen Daten des Betroffenen – das regelmäßig keinen Bezug zum konkreten Strafverfahren hat – nur so lange in den Unterlagen der Strafverfolgungsbehörden verbleiben, wie dies zur Strafverfolgung 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, deren biometrische Daten aus dem Strafverfahren für einen Abgleich mit im Internet öffentlich zugänglichen Daten nach § 98d StPO-E verwendet wurden, zu benachrichtigen ist. Dies kann der Beschuldigte oder ein Zeuge sein.

Zu Artikel 2 (Inkrafttreten)

Das Gesetz soll am Tag nach der Verkündung in Kraft treten. Den Strafverfolgungsbehörden sollen die neuen Befugnisse schnellstmöglich zur Verfügung stehen.