GESELLSCHAFT FÜR FREIHEITSRECHTE

2. April 2026

Stellungnahme der Gesellschaft für Freiheitsrechte e.V.

im Rahmen der Verbändebeteiligung

zum Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz „Entwurf eines Gesetzes zur Änderung der Strafprozessordnung – digitale Ermittlungsmaßnahmen"

A. Vorbemerkung

Der Referentenentwurf ist **zum Großteil verfassungswidrig**. Vor diesem Hintergrund sollte davon abgesehen werden, die darin vorgeschlagenen Ermittlungsmaßnahmen einzuführen. Mindestens muss der Entwurf aber an vielen Stellen geändert werden.

Der Referentenentwurf sieht eine **massive Ausweitung heimlicher Überwachungsbefugnisse** im Rahmen der Strafverfolgung vor. Bei den neuen Ermittlungsbefugnissen – automatisierte biometrische Abgleiche mit öffentlich verfügbaren Daten aus dem Internet sowie automatisierte verfahrensübergreifende Datenanalysen – handelt es sich um Instrumente, die zu **schwerwiegenden Grundrechtseingriffen** führen. Es handelt sich gerade nicht um gezielte Maßnahmen gegen einzelne tatverdächtige Personen, sondern um Instrumente zur potenziellen Massenüberwachung. Ziel sei, ausweislich der Entwurfsbegründung, eine Steigerung der Effektivität der Strafverfolgung. Allerdings liegen keinerlei Nachweise vor, die eine derartige Effektivitätssteigerung belegen. Vielmehr sind KI-Tools fehleranfällig und diskriminierend.

Besonders besorgniserregend ist, dass der Referentenentwurf staatliche **digitale Souveränität vollkommen ausblendet**. Biometrische Abgleiche im Internet sollen auch von privaten Anbieter*innen im Ausland durchgeführt werden dürfen. Damit soll den Sicherheitsbehörden wohl ermöglicht werden, Anbieter*innen wie PimEyes zu nutzen, deren Produkte mit unionsrechtlichen Vorgaben sowie den Grundrechten unvereinbar sind. Darüber hinaus soll auch im Rahmen der Datenanalysebefugnis der Einsatz von Softwaretools privater Anbieter wie z.B. Gotham des US-Unternehmens Palantir auf Grundlage des Entwurfs möglich sein. Der vorliegende Entwurf sieht keinerlei Vorgaben vor, die sensibelste Polizeidaten vor Fehlern, Datenlecks, unberechtigtem Zugriff, missbräuchlicher Nutzung oder Manipulation schützen.

Gesellschaft für Freiheitsrechte e.V.
Boyenstraße 41
10115 Berlin

info@freiheitsrechte.org
Amtsgericht Berlin-Charlottenburg
Registernummer VR 34505 B

GLS Gemeinschaftsbank eG
IBAN · DE 88 4306 0967 1182 9121 00
BIC · GENODEM1GLS

B. Bewertung im Einzelnen

Die einzelnen Befugnisse werfen eine Vielzahl gravierender verfassungs- und unionsrechtlicher Probleme auf.

1. Automatisierter biometrischer Abgleich mit öffentlich verfügbaren Daten aus dem Internet (§ 98d StPO-E)

a) Verfassungsrechtliche Bewertung

Die Befugnis genügt nicht den verfassungsrechtlichen Anforderungen. Diese richten sich an die Eingriffsschwelle und bei repressiven Maßnahmen an das Gewicht der Straftaten, die den Anlass der Überwachung bilden.[1] Das erforderliche Gewicht der verfolgten Straftat bestimmt sich maßgeblich nach der Eingriffsintensität. Es bedarf einer Gesamtschau der Kombination von Gewicht der Straftat und Stärke des Tatverdachts unter Berücksichtigung insbesondere der Intensität des Grundrechtseingriffs.[2]

§ 98d StPO-E ermöglicht schwerwiegende Eingriffe in das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG). Die Streubreite der Maßnahme ist enorm. Auch wenn die Befugnis den Aufbau einer umfassenden biometrischen Referenzdatenbank durch entsprechende Löschpflichten (§ 98d Abs. 3 StPO-E) ausschließt (der im Übrigen verfassungs- und unionsrechtlich unzulässig wäre), ermächtigt sie zu Eingriffen in die Grundrechte potenziell aller Menschen. Auch wenn diese selbst nicht Zielpersonen einer Maßnahme sind und keinen Anlass für Ermittlungsmaßnahmen gegeben haben, werden doch auch deren Grundrechte beeinträchtigt, da bei Abgleichen auch Nicht-Treffer Grundrechtseingriffe darstellen.[3] Einzelne Personen können nur begrenzt beeinflussen, ob zum Beispiel Bild- und Videomaterial oder Tonaufnahmen von ihnen gegen ihren Willen im Internet veröffentlicht werden. Erfasst sind auch solche Daten, die nach vorheriger Registrierung, Genehmigung oder Entgeltzahlung genutzt werden können[4], wie es typischerweise bei verschiedenen Sozialen Medien der Fall ist. Das Bundesverfassungsgericht hat mehrfach herausgestellt, dass biometrische Daten besonders schutzwürdig sind.[5] Außerdem können

[1] BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025, 1 BvR 180/23, Rn. 178.
[2] BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025, 1 BvR 180/23, Rn. 178.
[3] BVerfG, Beschluss des Ersten Senats vom 18. Dezember 2018, 1 BvR 142/15, Rn. 51
[4] Entwurfsbegründung, S. 12.
[5] BVerfG, Beschluss vom 18. Dezember 2018, 1 BvR 142/15, Rn. 53: „höchstpersönliche Merkmale wie das Gesicht"; vgl. auch BVerfG, Urteile des Ersten Senats vom16. Februar 2023, 1 BvR 1547/19 und 1 BvR 2634/20, Rn. 87.

Rückschlüsse auf besonders sensible Daten wie politische Einstellungen und sexuelle Orientierung gezogen werden (z.B. bei Aufnahmen von Demos, Parteiveranstaltungen, Gottesdiensten etc.). Anonymität im Internet, das einen erheblichen Teil des öffentlichen Raumes darstellt, wird damit faktisch unmöglich gemacht. Das ist mit enormen Abschreckungseffekten verbunden und hat erhebliche Auswirkungen auf die Ausübung von Grundrechten. Insbesondere die Ausübung der Meinungsfreiheit (Art. 5 Abs. 1 GG) über öffentliche Profile in Sozialen Medien wird damit besonders beeinträchtigt. Es ist auch nicht ausgeschlossen, dass Erkenntnisse aus dem Kernbereich privater Lebensgestaltung durch die Maßnahme erlangt werden. In diesem Zusammenhang ist beispielsweise an Dating Plattformen, sexualisierte Deep Fakes sowie an die Vielzahl sensibler Aufnahmen zu denken, die oftmals auch ohne Einverständnis der abgebildeten Personen erstellt und im Internet veröffentlicht werden. Die Systeme zum biometrischen Abgleich sind darüber hinaus höchst fehleranfällig und potentiell diskriminierend.[6] Wie das Bundesverfassungsgericht bereits ausgeführt hat, können mit einer weitergehenden Automatisierung von Polizeiarbeit spezifische Diskriminierungsrisiken einhergehen, die verfassungsrechtlich umso weniger hinzunehmen sind, je mehr sich die Wirkungen der automatisierten Datenanalyse oder -auswertung einer nach Art. 3 Abs. 3 GG unzulässigen Benachteiligung annähern könnten.[7] Eingriffsintensivierend wirkt zudem, dass die Abgleiche heimlich stattfinden und Rechtsschutzmöglichkeiten damit erheblich beschränkt sind. Darüber hinaus wirkt eingriffsverschärfend, dass nicht lediglich tatverdächtige Personen Zielperson der Befugnis sein können, sondern auch Zeug*innen. Berufsgeheimnisträger*innen sind von der Maßnahme nicht ausdrücklich ausgeschlossen. Immerhin ist ein Abgleich mit öffentlich zugänglichen Echtzeitdaten unzulässig (§ 98d Abs. 1 Satz 2 StPO-E).

Somit muss die vorgeschlagene Befugnis mindestens auf die Verfolgung besonders schwerer Straftaten beschränkt sein[8], um den verfassungsrechtlichen Anforderungen gerecht zu werden. Auch aus der Gesamtschau der Eingriffsvoraussetzungen, namentlich des qualifizierten Anfangsverdachts (§ 98d Abs. 1 Satz 1 Nr. 1 StPO-E) sowie des Subsidiaritätsvorbehalts (§ 98d Abs. 1 Satz 1 Nr. 2 StPO-E) ergibt sich keine Absenkung des erforderlichen Gewichts, wie das Bundesverfassungsgericht erst vor Kurzem festgestellt hat.[9] § 98d Abs. 1 Satz 1 Nr. 1 StPO-E lässt aber „Straftat[en] von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Absatz 2 StPO bezeichnete Straftat“ ausreichen. Diese Voraussetzung erfüllt in mehrerlei Hinsicht

[6] Vgl. insb. zur Auswirkung von Fehleranfälligkeit und Diskriminierungsgefahr auf die Eingriffsintensität, Datenanalyseurteil Rn. 90.
[7] Vgl. BVerfG, Urteile des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19 und 1 BvR 2634/20, Rn. 77.
[8] Ausführlich zu den Voraussetzungen besonders schwerer Straftaten BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025, 1 BvR 180/23, Rn. 209 ff.
[9] BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025, 1 BvR 180/23, Rn. 205.

nicht die verfassungsrechtlichen Anforderungen. Erstens genügen „erhebliche Straftaten" nicht dem verfassungsrechtlich notwendigen Gewicht einer besonders schweren Straftat. Zweitens werden die erfassten Straftaten nicht hinreichend konkretisiert. Der Gesetzgeber muss dafür entweder auf bestehende Kataloge zurückgreifen oder einen eigenen Katalog schaffen.[10] Eine Generalklausel oder lediglich die abstrakte Verweisung auf Straftaten von besonderer Schwere reichen nicht aus.[11] Diese Anforderung ist nicht erfüllt, wenn der Gesetzgeber, wie vorliegend, abstrakt an „Straftat[en] von auch im Einzelfall erheblicher Bedeutung" anknüpft und lediglich teilweise („insbesondere") auf einen Katalog verweist. Das ist auch nicht mit dem Grundsatz der Bestimmtheit und Normenklarheit vereinbar. Drittens hat das Bundesverfassungsgericht bereits festgestellt, dass ein erheblicher Teil der in § 100a Abs 2 StPO genannten Straftaten nicht die Voraussetzungen von besonders schweren Straftaten erfüllen.[12] Insofern genügt auch im Rahmen des § 98d StPO-E kein Verweis auf § 100a Abs. 2 StPO.

Die Befugnis sieht außerdem nur wenige flankierende Schutzvorkehrungen vor. Diese sind auch aufgrund von Art. 10 JI-RL geboten. Die Protokollierungspflicht (§ 98d Abs. 2 StPO-E) ist grundsätzlich zu begrüßen, um überhaupt Anknüpfungspunkte für eine datenschutzrechtliche Kontrolle zu haben, gewährleistet allein aber keinesfalls eine effektive Kontrolle. § 98d Abs. 4 StPO-E sieht vor, dass Abgleiche grundsätzlich durch die Staatsanwaltschaft angeordnet werden müssen. Angesichts der Eingriffstiefe wäre eine unabhängige gerichtliche Kontrolle geboten. Positiv zu bewerten ist die Benachrichtigungspflicht nach § 101 Abs. 1a StPO-E. Mit Blick darauf, dass auch Zeug*innen Ziel der Maßnahme sein können, ist diese aber auch geboten, da für Zeug*innen Rechtsschutz mangels Kenntnis sonst unmöglich wäre.

b) Verbleibende praktische Anwendungsfälle ohne Datenbankaufbau

Art. 5 Abs. 1 lit. e KI-VO verbietet insbesondere die Verwendung von KI-Systemen, die Datenbanken zur Gesichtserkennung durch das ungezielte Auslesen von Gesichtsbildern aus dem Internet erstellen oder erweitern. Auch verfassungsrechtlich wäre der Aufbau einer Referenzdatenbank auf Vorrat unzulässig. Vor diesem Hintergrund schließt der Entwurf richtigerweise den Aufbau einer biometrischen Referenzdatenbank auf Vorrat aus, indem er eine Löschverpflichtung enthält (Abs. 3).

Wie ein Gutachten aus dem letzten Jahr eindrücklich zeigt, ist es aus technischen Gründen aber praktisch unmöglich, für jede einzelne Abgleichmaßnahme den gesamten Datenbestand im

[10] BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025, 1 BvR 180/23, Rn. 208.
[11] BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025, 1 BvR 180/23, Rn. 208, 214.
[12] BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025, 1 BvR 180/23, Rn. 213 ff.

Internet erneut zu durchsuchen.[13] Dies würde schlichtweg sehr lange dauern. Deshalb arbeiten auch Suchmaschinen mit Datenbanken. Lediglich Daten aus beispielsweise öffentlichen Facebook-Gruppen oder öffentlichen Channels könnten damit abgeglichen werden. Damit ist der praktische Anwendungsbereich der Befugnis sehr klein und der Effektivitätsgewinn dürfte sich in Grenzen halten.

Da unter öffentlich zugängliche Daten auch solche Daten fallen, deren Nutzung eine Registrierung erfordert oder für die bezahlt werden muss, ist der Rückgriff auf kommerzielle Angebote grundsätzlich von der Befugnis erfasst. Somit wäre den Behörden auch die Nutzung der biometrischen Datenbanken von Privatanbieter*innen wie PimEyes oder Clearview AI erlaubt. Anbieter*innen wie PimEyes verstoßen sowohl gegen das Scraping-Verbot der KI-Verordnung als auch gegen Datenschutzrecht. Beispielweise hat der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg ein Bußgeldverfahren eröffnet.[14] Ein Rückgriff auf rechtswidrige Angebote Privater ist für den Staat, der gemäß Art. 20 Abs. 3 GG an Gesetz und Recht gebunden ist, aber ausgeschlossen.

c) Rückgriff auf private Anbieter*innen in Drittstaaten

Wohl im Bewusstsein dieses sehr kleinen verbleibenden praktischen Anwendungsfeldes offenbaren die Verfasser*innen des Entwurfs in der Entwurfsbegründung, dass es – für den Fall, dass die Strafverfolgungsbehörden den Abgleich technisch nicht selbst durchführen können – möglich sein soll, über die justizielle Rechtshilfe auf Anbieter*innen im Ausland zuzugreifen.[15] Für die Staatsanwaltschaften bestehe daneben die Möglichkeit, an das Bundeskriminalamt in seiner Zentralstellenfunktion heranzutreten, das wiederum im Wege der sogenannten polizeilichen Rechtshilfe an ausländische Stellen herantreten könnte.[16] Dies soll wiederum über den neuen § 9a BKAG-E erfolgen, der im Referentenentwurf des Bundesministeriums des Inneren[17] vorgeschlagen wird. Dieser Entwurf sieht explizit die Inanspruchnahme privater Anbieter in Drittstaaten außerhalb der EU vor.[18] Damit wird eine spezialgesetzliche Regelung eingeführt, um

[13] Lewandowski, Braucht die Polizei eine Datenbank zum biometrischen Abgleich? Das Durchsuchen von Internetbildern zur Gesichtserkennung, September 2025, abrufbar unter https://algorithmwatch.org/de/wp-content/uploads/2025/10/2025-AW-Gutachten-V9.pdf (abgerufen am 2.4.2026).
[14] PimEyes: LfDI eröffnet Bußgeldverfahren, 21. Dezember 2022, abrufbar unter https://www.baden-wuerttemberg.datenschutz.de/pimeyes-lfdi-eroeffnet-bussgeldverfahren/ (abgerufen am 2.4.2026).
[15] Entwurfsbegründung, S. 13.
[16] Entwurfsbegründung, S. 13.
[17] Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit.
[18] Entwurfsbegründung, S. 13.

die Umgehung der für den Staat geltenden rechtlichen Anforderungen zu ermöglichen.[19] Selbst wenn kommerzielle Datenbanken im Ausland legal erstellt würden, da sie nicht den Vorgaben der KI-VO und DSGVO unterliegen, dürfte der Staat die für ihn geltenden rechtlichen Grenzen nicht umgehen, indem er auf diese Anbieter zurückgreift. In diesem Sinne hat das Bundesverfassungsgericht (für die Zusammenarbeit mit ausländischen Nachrichtendiensten) betont, dass dem solchen Praktiken inhärenten Potential einer Umgehung innerstaatlicher Bindungen und den spezifischen Grundrechtsgefährdungen, die durch die Zusammenarbeit eintreten können, Rechnung zu tragen ist.[20] Die Grenzen der inländischen Datenerhebung und -verarbeitung des Grundgesetzes dürfen durch einen Austausch von Daten nicht in ihrer Substanz unterlaufen werden.[21] Auch der EGMR fordert, dass Rechtsgrundlagen soweit wie möglich Umgehungen verhindern müssen.[22] Entsprechend müssen auch die Vorschriften zur internationalen justiziellen Rechtshilfe interpretiert werden.

d) Änderungsbedarf

Vor diesem Hintergrund sollten mindestens folgende Anpassungen erfolgen:

- Es sollte ausschließlich und abschließend an den Katalog des **§ 100b Abs. 2 StPO** angeknüpft werden.
- **Zeug*innen** sollten als Zielpersonen gestrichen werden, mindestens muss ein Schutz von **Berufsgeheimnisträger*innen** vorgesehen werden.
- Es sollte ein **Kernbereichsschutz** verankert werden; dazu könnte an § 100d Abs. 1-5 StPO angeknüpft werden.
- Es sollte ein **Beweisverwertungsverbot** für Erkenntnisse aus rechtswidrig durchgeführten Maßnahmen und darauf beruhenden weitere Erkenntnissen verankert werden (Beweisverwertungsverbot mit Fernwirkung).
- Die **Einbindung der zuständigen Datenschutzbeauftragten** muss angesichts der datenschutzrechtlichen Risiken ausgeweitet werden: Es müssen verpflichtende regelmäßige Kontrollen vorgeschrieben werden. Außerdem sollte eine Ermächtigungsgrundlage für den Erlass einer Rechtsverordnung eingeführt werden, die das Nähere zum technischen Verfahren sowie Schutzvorkehrungen enthalten muss und das Einvernehmen mit der BfDI voraussetzt.

[19] Siehe dazu die Stellungnahme der GFF vom 2. April 2026 zu den Referentenentwürfen des BMI.
[20] BVerfG, Urteil des Ersten Senats vom 19. Mai 2020, 1 BvR 2835/17, Rn. 250 mit Verweis auf EGMR.
[21] Vgl. BVerfG, Urteil des Ersten Senats vom 20. April 2016, 1 BvR 966/09 und 1 BvR 1140/09, Rn. 327 zur Übermittlung an eine ausländische staatliche Stelle.
[22] Vgl. EGMR, Big Brother Watch and others v. United Kingdom, Urteil vom 13. September 2018, Nr. 58170/13 u.a., Rn. 424.

- Es sollte klargestellt werden, dass die vorgesehene **Protokollierung auch aktenkundig** gemacht werden muss.
- Weiterhin sollte ein **Gerichtsvorbehalt** eingeführt werden. Es sollten außerdem Mindestvorgaben für den Antrag und die gerichtliche Entscheidung gesetzlich geregelt werden.
- Ein Abgleich durch private Anbieter*innen in Drittstaaten sollte gesetzlich ausgeschlossen werden. Dazu sollte im Normtext verankert werden, dass **Auftragsverarbeiter*innen ihren Sitz ausschließlich innerhalb der Europäischen Union**, einschließlich der Schengen-assoziierten Staaten, haben dürfen und personenbezogene Daten nur an solche Personen übermittelt werden, die Amtsträger*innen oder für den öffentlichen Dienst besonders Verpflichtete sind oder die zur Geheimhaltung verpflichtet worden sind.

Gesellschaft für Freiheitsrechte e.V.
Boyenstraße 41
10115 Berlin

info@freiheitsrechte.org
Amtsgericht Berlin-Charlottenburg
Registernummer VR 34505 B

GLS Gemeinschaftsbank eG
IBAN · DE 88 4306 0967 1182 9121 00
BIC · GENODEM1GLS

2. Automatisierte verfahrensübergreifende Datenanalyse (§ 98e StPO-E)

Der Entwurf sieht in § 98e StPO-E außerdem eine Befugnis zur automatisierten Datenanalyse für die Strafverfolgungsbehörden vor.

a) Datenanalysen als Gefahr für die Grund- und Menschenrechte

Mit automatisierten Datenanalysen können große Mengen auch bislang ungefilterter oder getrennt gespeicherter Daten in kürzester Zeit mit weiteren Daten verbunden und verarbeitet werden, um so „neues Wissen zu generieren".[23] Ziel ist gerade, dass durch automatisierte technische Prozesse Erkenntnisse gewonnen werden, die den Ermittlungspersonen noch nicht bekannt waren. Bei hochkomplexen Analysealgorithmen sind deren Ergebnisse für die Anwender*innen dabei nicht nachvollziehbar („Blackbox"). Es werden unüberschaubare, teils ungefilterte Mengen sensibler Daten aus Gefahrenabwehr oder Strafverfolgung zusammengeführt und mit komplexen Algorithmen analysiert, wobei auch weitgehende Sachverhaltsbewertungen und Profilerstellungen (Profiling) und damit automatisierte Ermittlungen in Form von „predictive policing" möglich sind. Dabei besteht die Gefahr, dass aufgrund von Fehlern im Analyseprogramm, insbesondere aufgrund diskriminierender Algorithmen, Menschen fälschlicherweise ins Visier der Sicherheits- und Strafverfolgungsbehörden geraten, obwohl sie dafür keinen Anlass geboten haben. Allein die heimliche automatisierte Verarbeitung von gespeicherten Daten greift bereits tief in die Grundrechte der Bürger*innen ein. Noch intensiver sind die Auswirkungen auf die Grundrechte aber, wenn aufgrund der Analysen behördliche Eingriffe wie Überwachungsmaßnahmen, Durchsuchungen oder Festnahmen erfolgen. Schon das Wissen darum, dass eigene bei Polizei und Staatsanwaltschaft gespeicherte Daten in solche Analysetools geraten (könnten), entfaltet zudem schwere Einschüchterungseffekte und kann ein Gefühl der dauerhaften Überwachung erzeugen. Gleichzeitig liegen keine Statistiken zur Wirksamkeit von und belastbare Zahlen zu Ermittlungserfolgen durch polizeiliche Datenanalysen vor, obwohl in Bundesländern wie Hessen und Nordrhein-Westfalen Analysetools schon seit Jahren zum Einsatz kommen.

Datenanalysekompetenzen dürfen zudem nicht isoliert betrachtet werden. Vielmehr ist zu berücksichtigen, dass durch immer stärkere Überwachungs- und Ermittlungsbefugnisse auch immer mehr und immer sensiblere Daten in den Polizeidatenbanken gespeichert werden. Dies gilt besonders für biometrische Überwachungsbefugnisse, wie sie in diesem Entwurf ebenfalls vorgesehen sind. Automatisierte Datenanalysen sind mächtige Überwachungsmaßnahmen. Wenn solche ermöglicht werden sollen, ist eine strenge Beschränkung zum Schutz der

[23] Vgl. BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19 und 1 BvR 2634/20, Rn. 67.

Grundrechte unerlässlich. Der Einsatz von Datenanalysetools in anderen Staaten (aktuell der Einsatz von Palantir Gotham und anderer Software durch die US-Behörden wie ICE[24]) und auch in militärischen Konflikten[25] zeigt, wie weitgehende Überwachung und auch Steuerung staatlichen Handelns diese Tools ermöglichen. Angesichts der mit sog. Datamining verbundenen Risiken und Gefahren für Grund- und Menschenrechte muss die Befugnis im vorliegenden Entwurf eingeschränkt werden.

Die Datenanalyse sollte dabei insbesondere ausdrücklich auf **einfach-automatisierte Abgleiche und reine Suchvorgänge** begrenzt werden. Algorithmische Sachverhaltsbewertungen, Profiling und KI-basierte Analysen müssen ausgeschlossen werden. Die Menge der einbezogenen Daten ist stark zu begrenzen. Die Eingriffsschwellen für automatisierte Datenanalysen müssen erhöht und Schutzmaßnahmen gegen Fehler, Diskriminierung und Intransparenz aufgenommen werden.

b) Nichteinhaltung der verfassungsrechtlichen Anforderungen

Die verfassungsrechtlichen Anforderungen an derartige Ermächtigungsgrundlagen ergeben sich aus dem Datenanalyseurteil des Bundesverfassungsgerichts,[26] in dem das Gericht über Rechtsgrundlagen zur polizeilichen Datenanalyse zum Zwecke der Gefahrenabwehr entschied. § 98e StPO-E bleibt hinter den verfassungsrechtlich erforderlichen Voraussetzungen zurück.

aa) Hohes Eingriffsgewicht

Die Befugnisnormen ermöglichen schwerwiegende Eingriffe in Art. 10 GG, das Recht auf informationelle Selbstbestimmung und das IT-System-Grundrecht (jeweils Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG). Die ermöglichten Datenanalysen sind nicht ausreichend gesetzlich beschränkt, um das Eingriffsgewicht zu verringern.

[24] Dazu insbesondere „Mit Palantir und Paragon auf Migrantenjagd“, netzpolitik.org (Monroy) vom 17. Januar 2026, https://netzpolitik.org/2026/us-einwanderungsbehoerde-mit-palantir-und-paragon-auf-migrantenjagd/.
[25] Dazu insbesondere „"Targeting": Palantir unterstützt die Ukraine bei der Kriegsführung“, heise.de (Mewes) vom 2. Februar 2023, https://www.heise.de/news/Targeting-Palantir-unterstuetzt-die-Ukraine-bei-der-Kriegsfuehrung-7481072.html sowie ein Werbeclip des Unternehmens Palantir zu seiner Software Gotham, https://www.youtube.com/watch?v=rxKghrZU5w8.
[26] BVerfG, Urteile des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19 und 1 BvR 2634/20.

§ 98e StPO-E enthält keine ausreichenden Einschränkungen in Bezug auf Art und Umfang der Daten sowie hinsichtlich der Methode der Datenverarbeitung, die das Eingriffsgewicht verringern könnten.[27]

Dabei ist zwar grundsätzlich zu begrüßen, dass der Entwurf immerhin die Daten, die in die Datenanalysen einfließen können, abschließend benennt. Allerdings sind Vorgangsdaten und Daten aus dem polizeilichen Informationsaustausch grundsätzlich in die Analyse mit einbezogen. Asservaten und Daten aus eingriffsintensiven Maßnahmen wie Telekommunikationsüberwachungen können ergänzend einbezogen werden. So sind nach dem Entwurf riesige Mengen auch sensibler Daten analysefähig. Dabei sind in großem Umfang auch Daten unbeteiligter und bislang unverdächtiger Personen wie insbesondere Zeug*innen, Anzeigeerstatter*innen und Betroffene von Straftaten umfasst.[28] Besonders sensible Datenarten wie biometrische Daten, genauso wie Fotos und Videos, Tonaufnahmen oder Telekommunikations- oder Standortdaten sind nicht ausgenommen.

Auch die ermöglichten Analysemethoden sind sehr weitgehend. Insbesondere sind keinerlei methodische Einschränkungen zum Einsatz selbstlernender Systeme oder anderer Formen künstlicher Intelligenz enthalten, was das Eingriffsgewicht der Maßnahmen deutlich verschärft.[29] § 98e StPO-E ermöglicht damit auch umfassende Sachverhaltsanalysen, die Erstellung von Personenprofilen und predictive policing.[30] Solche Analysemethoden bedürfen besonders strengen Voraussetzungen für eine verfassungsrechtliche Rechtfertigung.[31]

bb) Unzureichende Eingriffsschwellen

Nach den Maßstäben des Bundesverfassungsgerichts aus dem im Datenanalyse-Urteil handelt es sich folglich um schwerwiegende Grundrechtseingriffe. Befugnisse zur Durchführung von Datenanalysen, die sich als besonders schwerwiegende Grundrechtseingriffe darstellen, sind nur unter den engen Voraussetzungen zu rechtfertigen, die das Bundesverfassungsgericht allgemein für eingriffsintensive heimliche Überwachungsmaßnahmen entwickelt hat.[32] Die vorgesehenen Anforderungen an einen Einsatz der automatisierten Datenanalyse zur Strafverfolgung genügen

[27] Vgl. BVerfG, Urteile des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19 und 1 BvR 2634/20, Rn. 78 ff., 90 ff.
[28] Siehe auch Entwurfsbegründung, S. 16.
[29] Vgl. BVerfG, Urteile des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19 und 1 BvR 2634/20, Rn. 100, 101.
[30] Vgl. BVerfG, Urteile des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19 und 1 BvR 2634/20, Rn. 98.
[31] Vgl. BVerfG, Urteile des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19 und 1 BvR 2634/20, Rn. 121.
[32] Vgl. BVerfG, Urteile des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19 und 1 BvR 2634/20, Rn. 104 ff.

nicht, um die damit einhergehenden schwerwiegenden Grundrechtseingriffe zu rechtfertigen. Insoweit verletzen die geplanten Befugnisse Art. 10 GG sowie das allgemeine Persönlichkeitsrecht und das IT-System-Grundrecht (jeweils Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG).

Schwerwiegende Grundrechtseingriffe zur Strafverfolgung sind nur zur Aufklärung besonders schwerer Straftaten zulässig. Jedoch knüpft § 98e StPO-E an den Katalog des § 100a Abs. 2 StPO an. Für diesen hat das Bundesverfassungsgericht in seiner Trojaner-II-Entscheidung jedoch 2025 festgestellt, dass dieser gerade nicht nur besonders schwere Straftaten enthält.[33]

cc) Fehlen von flankierenden Schutzmaßnahmen und zureichender Kontrolle

Darüber hinaus fehlt es in § 98e StPO-E an Regelungen, die den verfassungskonformen und rechtmäßigen Betrieb der Datenanalyseplattformen tatsächlich im Einsatz sichern. Da die Befugnisse den Einsatz komplexer Systeme und auch statistische Auswertungen erlauben, bedarf es Vorkehrungen gegen eine hiermit spezifisch verbundene Fehler- und Diskriminierungsanfälligkeit und zur Sicherung der Nachvollziehbarkeit.[34]

In Frage kommen u.a. Vorgaben zu Ausgewogenheit und Qualität von Trainingsdaten[35] sowie zu Analysekriterien (insbesondere zu Proxys, also diskriminierenden Stellvertreterkriterien)[36]. Ebenso denkbar sind Transparenzmaßnahmen wie Tests[37] und Vorgaben zur Erklärbarkeit von Analyseergebnissen[38] sowie Regeln zur Entscheidungsfindung aufgrund von Analyseergebnissen (Vermeidung von sog. automation biases).[39] Hierzu muss der Gesetzgeber konkrete praktische Maßnahmen vorsehen oder zumindest anleiten. Solche Vorkehrungen sind besonders wichtig, da der Entwurf technologieoffen ausgestaltet ist und auch der Einsatz von Tools und Software privater Unternehmen mit Sitz außerhalb der EU möglich ist.

---

[33] Vgl. BVerfG, Beschluss des Ersten Senats vom 24. Juni 2025, 1 BvR 180/23, Rn. 213 ff.
[34] Vgl. BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19 und 1 BvR 2634/20, Rn. 95, 100, 101, 109.
[35] *Hüger*, Künstliche Intelligenz und Diskriminierung, 2023, S. 158 ff. m.w.N.; *Lauscher/Legner*, ZfDR 2022, 367, (371).
[36] Dazu *Rabe* in: Bäuerle/Denker/Geminn et al, KI und Big Data bei der Polizei, 2025, S. 15 (39 f.); *Beck*, Künstliche Intelligenz und Diskriminierung, 2019, S. 17; *Buchholtz/Scheffel-Kain*, NVwZ 2022, 612 ff.; *Tinhofer*, DRdA 1a/2022, Heft 399, 170 (174 ff.).
[37] Dazu insbesondere *Hüger*, Künstliche Intelligenz und Diskriminierung, 2023, S. 153 ff. m.w.N.
[38] Dazu insbesondere *Ibold,* GSZ 2024, 10 (15 f.).
[39] Dazu insbesondere *Rabe* in: Bäuerle/Denker/Geminn et al, KI und Big Data bei der Polizei, 2025, S. 15 (34); zum Begriff näher *Ruschemeier* in: Proceedings of the Weizenbaum Conference 2023: AI, Big Data, Social Media, and People on the Move, 2023, S. 1 (4).

Zudem bedarf es der Anordnung konkreter Maßnahmen, um die Einhaltung des Zweckbindungsgrundsatzes auch praktisch sicherzustellen.[40]

Abstrakte Gebote wie § 98e Abs. 4 Satz 5 StPO-E, nach denen sicherzustellen ist, dass diskriminierende Algorithmen weder herausgebildet noch verwendet werden, genügen gerade nicht zur praktischen Durchsetzung. Erforderlich wäre wenigstens ein verbindlicher hinreichend bestimmter Auftrag an die Verwaltung zur Ausarbeitung entsprechender Konzepte und zu deren Veröffentlichung.[41] Ebenso wenig genügt § 98e Abs. 6 StPO-E, da keinerlei konkrete technische und organisatorische Maßnahmen angeleitet werden, die die Wahrung der Zweckbindungsgrundsätze tatsächlich und normenklar sichern.

Ebenfalls müssen regelmäßige, verdachtsunabhängige Kontrollen der Datenanalysepraxis durch interne und externe Datenschutzbeauftragte vorgesehen werden,[42] die mindestens alle zwei Jahre erfolgen.[43]

Es wird außerdem darauf hingewiesen, dass beim Einsatz selbstlernender und sonstiger KI-Systeme auch die Vorgaben für Anbieter*innen aus der KI-VO eingehalten werden müssen, wenn die Behörde die KI-Systeme mit ihrem Namen versieht oder wesentliche Veränderungen an ihnen vornimmt, Art. 25 Abs. 1 lit. a, b KI-VO („Quasi-Anbieter").[44] Darüber hinaus finden die Vorgaben der KI-VO bislang noch keine unmittelbare Anwendung.[45] Jedenfalls bis zu deren unmittelbarer Geltung muss der Gesetzgeber selbst ausreichende Schutzmaßnahmen vorsehen.

c) Besonderes Risiko bei Software privater Anbieter*innen

Jedenfalls sollte zur Ausübung der Befugnisse nicht auf die Softwareangebote privater Unternehmen zurückgegriffen werden. Anderenfalls können Manipulation, unbefugte Datenzugriffe und Leaks nicht ausgeschlossen werden. Es drohen Abhängigkeiten des Staates von privaten Anbieter*innen, die – in faktischen Monopolstellungen – Preise und Nutzungsbedingungen frei diktieren können. Auch bei einer Nutzung als „Übergangslösung" besteht das Risiko von Lock-In-Effekten, die einen Wechsel zu einer anderen Lösung erschweren.

[40] Vgl. BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19 und 1 BvR 2634/20, Rn. 118.
[41] Vgl. BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19 und 1 BvR 2634/20, Rn. 118.
[42] Vgl. BVerfG, Urteil des Ersten Senats vom 16. Februar 2023, 1 BvR 1547/19 und 1 BvR 2634/20, Rn. 109.
[43] Vgl. BVerfG, Urteil des Ersten Senats vom 20. April 2016, 1 BvR 966/09, 1 BvR 1140/09, Rn. 141.
[44] Vgl. *Martini/Botta*, DÖV 2025 1033 (1037 f.).
[45] Die Bestimmungen zum Umgang mit Hochrisiko-KI-Systemen werden frühestens am 2. August 2027 wirksam, Art. 113 Abs. 3 lit. c KI-VO, so nicht durch den aktuell vorliegenden Verordnungsvorschlag „Digital Omnibus on AI" ein noch späterer Zeitpunkt des Inkrafttretens festgesetzt wird.

Bei außereuropäischen Anbieter*innen ist zudem die Rechtsdurchsetzung deutscher und europäischer Schutzvorschriften bei Vertragsverletzungen wie Datenleaks und unbefugten Datenzugriffen nicht gewährleistet. Aus diesen Gründen hat sich die Bundesministerin der Justiz und für Verbraucherschutz 2026 gegen eine Lizensierung von Analysesoftwareprodukten des US-Anbieters Palantir ausgesprochen.[46] Die Bundesregierung gibt an, bislang keine Entscheidung über die Beschaffung bestimmter Softwarelösungen zur Auswertung und Analyse für Bundespolizei und BKA getroffen zu haben.[47]

Der Entwurf enthält jedoch keinerlei Vorgaben zur Sicherung der staatlichen digitalen Souveränität. Auch der Einsatz von Softwaretools privater Anbieter wie z.B. Gotham des US-Anbieters Palantir wäre auf Grundlage des Entwurfs möglich.

Aufgrund des Wesentlichkeitsgrundsatzes und der hohen Bedeutung für die Grundrechte der Bürger*innen ist zu fordern, dass der Gesetzgeber Anforderungen an die Anbieter*innen und ihre angebotenen Analyseprogramme im Gesetz zumindest in Grundzügen vorgibt. Festzuschreiben wäre, dass die genutzten Tools transparent sein müssen. Dazu erforderlich ist, dass der Quellcode vor Inbetriebnahme und vor Updates zur umfassenden Prüfung zur Verfügung steht. Nur so kann eine verfassungs- und europarechtskonforme Datenanalysepraxis sichergestellt werden. Zudem muss ausgeschlossen sein, dass Analysetools außereuropäischer Anbieter*innen zum Einsatz kommen, damit nationales und europäisches Recht sicher durchgesetzt werden kann. Als Analysetools kommen in diesem Falle insbesondere öffentliche Softwareprogramme (beispielsweise nach Entwicklung in einem europäischen Verbund) in Betracht.

d) Anpassungsbedarf

Vor diesem Hintergrund sollten mindestens folgende Anpassungen erfolgen:

- Die Datenanalyse sollte auf **einfach-automatisierte Abgleiche und reine Suchvorgänge** begrenzt werden. **Algorithmische** Sachverhaltsbewertungen, Profiling und KI-basierte Analysen sollten **ausgeschlossen** werden.

[46] „Einführung der bundesweiten Nutzung von Palantir wird es mit SPD nicht geben“, Welt.de (Breyton, Woldin, Fürsen), 23. Januar 2026, https://www.welt.de/politik/deutschland/article696dec0d173ea7f40d17cd3d/umstrittene-polizei-software-einfuehrung-der-bundesweiten-nutzung-von-palantir-wird-es-mit-spd-nicht-geben.html.

[47] BT-Drs. 21/4923 (Antwort der Bundesregierung. auf die Kleine Anfrage der Abgeordneten Ruben Rupp, Robin Jünger, Alexander Arpaschi, weiterer Abgeordneter und der Fraktion der AfD – Drucksache 21/4599 – Zum möglichen Einsatz der Software der Firma Palantir bei der Bundespolizei und beim Bundeskriminalamt), S. 2.

- Es sollte an den Katalog des **§ 100b Abs. 2 StPO** angeknüpft werden. Zusätzlich sollte an die tatsächlich erfolgte **Verletzung besonders gewichtiger Rechtsgüter** angeknüpft werden.
- Es müssen effektive, technisch-organisatorische **Vorkehrungen zur Vermeidung von Fehlern und Diskriminierung, sowie zur Einhaltung der Zweckbindung** getroffen werden. Dafür ist ein verbindlicher hinreichend bestimmter Auftrag an die Verwaltung zur Ausarbeitung entsprechender Konzepte und zu deren Veröffentlichung im Gesetz notwendig.
- Es sollte ein **Beweisverwertungsverbot** für Erkenntnisse aus rechtswidrig durchgeführten Maßnahmen und darauf beruhenden weiteren Erkenntnissen verankert werden (Beweisverwertungsverbot mit Fernwirkung).
- Die **Einbindung der zuständigen Datenschutzbeauftragten** sollte angesichts der datenschutzrechtlichen Risiken ausgeweitet werden: Es müssen verpflichtende regelmäßige Kontrollen vorgeschrieben werden.
- Im Lichte digitaler Souveränität sollten im Gesetz selbst **Vorgaben zur Transparenz der eingesetzten Tools** und **Anforderungen an die Anbieter*innen möglicherweise genutzter Tools** festgeschrieben werden.

Kontakt:

Dr. Simone Ruf
Stellvertretende Leitung Center for User Rights
simone.ruf@freiheitsrechte.org
PGP Key ID 0x9FE452FA136F5C9F