Wirtschaftsstrafrechtliche Vereinigung e.V. | Neusser Str. 99 | 50670 Köln

Bundesministerium der Justiz und
für Verbraucherschutz
Anton-Wilhelm-Amo-Straße 37
10117 Berlin

Wirtschaftsstrafrechtliche Vereinigung e.V.
Geschäftsstelle: Niklas Witt u. Natalie Witt
Neusser Str. 99
50670 Köln
Fon: +49 (221) 912645-0
Fax: 0221/912645-45
geschaeftsstelle@wistev.de

Köln, den 01.04.2026

Geschäftszeichen: 411224#00001#0008

Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz „Entwurf eines Gesetzes zur Änderung der Strafprozessordnung – Digitale Ermittlungsmaßnahmen“

Sehr geehrte Damen und Herren,

die Wirtschaftsstrafrechtliche Vereinigung e.V. (WisteV) bedankt sich für die Gelegenheit, zu dem Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz für ein „Gesetz zur Änderung der Strafprozessordnung – Digitale Ermittlungsmaßnahmen“ Stellung nehmen zu dürfen und nimmt diese Gelegenheit in Bezug auf die strafrechtlichen Implikationen gerne wahr.

Der vorliegende Referentenentwurf des BMJV verfolgt das grundsätzlich legitime Ziel, den Strafverfolgungsbehörden gesetzliche Grundlagen für den Einsatz digitaler Ermittlungsinstrumente zu schaffen, die sowohl das Bundesverfassungsgericht in seiner

Palantir-Entscheidung vom 16. Februar 2023 (1 BvR 1547/19 u.a.) als auch die KI-Verordnung der EU einfordern. Gleichwohl weist der Entwurf in seiner derzeitigen Fassung erhebliche verfassungsrechtliche, europarechtliche und rechtsstaatliche Defizite auf, die einer grundlegenden Überarbeitung bedürfen.

§ 98d und § 98e StPO-E sollen zwar nur bei Straftaten von auch im Einzelfall erheblicher Bedeutung, insbesondere in denen in § 100a Absatz 2 bezeichnete Straftaten anwendbar sein; dies dürfte primär bei Ermittlungen im Bereich der Kapitaldelikte und Delikte der organisierten Kriminalität der Fall sein. Allerdings sind Ermittlungsmaßnahmen auf Basis der geplanten Vorschriften auch in bestimmten Fällen schwerer Wirtschaftskriminalität möglich, so dass sich WisteV e. V. zu einer Stellungnahme veranlasst sieht.

Im Kern betreffen die Bedenken die folgenden zwölf Regelungskomplexe: das Fehlen eines Richtervorbehalts für beide Maßnahmen, die unbestimmte Eingriffsschwelle bei § 98d StPO-E, unzureichende Kernbereichs- und Berufsgeheimnisschutzregelungen, die fehlende normtextliche Begrenzung biometrischer Referenzdatenbanken und deren europarechtliche Problematik, eine zu weite Definition der „öffentlich zugänglichen Daten“, unzureichende technisch-organisatorische Sicherungsvorgaben, fehlende Begrenzungen der KI-Analysemethodik bei § 98e StPO-E, das Fehlen einer eigenständigen Zufallsfundregelung, die fehlende Zweckbeschränkung des biometrischen Abgleichs auf Personenfahndung und -identifizierung, die unzureichende Umsetzung der unionsrechtlichen Erforderlichkeitsschwelle aus Art. 10 der Richtlinie (EU) 2016/680, das fehlende Auffindeverdacht-Erfordernis bei der verfahrensübergreifenden Datenanalyse sowie unzureichende Dokumentations- und Reproduzierbarkeitspflichten.

I. Richtervorbehalt für § 98d und § 98e StPO-E

Der Entwurf sieht für den biometrischen Internetabgleich nach § 98d StPO-E lediglich eine Anordnungskompetenz der Staatsanwaltschaft vor (Abs. 4), bei Gefahr im Verzug sogar der Ermittlungspersonen. Für die automatisierte verfahrensübergreifende Datenanalyse nach § 98e StPO-E fehlt jegliche ausdrückliche Anordnungsregelung.

Dies ist mit der strafprozessualen Systematik bei vergleichbar eingriffsintensiven Maßnahmen nicht vereinbar. Der Entwurf selbst verortet die Eingriffsintensität des biometrischen Abgleichs auf dem Niveau der §§ 100g, 100i StPO. Bei einer Gesamtbetrachtung

des Eingriffsgewichts – insbesondere unter Berücksichtigung der Streubreite der Maßnahme, die potentiell Millionen unbeteiligter Internetnutzer betrifft – liegt die Eingriffsintensität deutlich über derjenigen einer Telekommunikationsüberwachung, die dem Richtervorbehalt des § 100e StPO unterliegt.

Für § 98e StPO-E ergibt sich das Erfordernis eines Richtervorbehalts unmittelbar aus der Palantir-Entscheidung des Bundesverfassungsgerichts (BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19, 1 BvR 2634/20). Dort hat das Gericht das Eingriffsgewicht verfahrensübergreifender Analyseplattformen als „potenziell sehr hoch“ eingestuft, vergleichbar mit tief in die Privatsphäre eingreifenden Überwachungsmaßnahmen – worunter nach dem BVerfG auch die Telekommunikationsüberwachung fällt (BVerfG, Beschluss vom 24. Juni 2025 – 1 BvR 180/23 –, Rn. 197).

Beide Normen sollten daher um einen Richtervorbehalt ergänzt werden. Für § 98d StPO-E sollte die Anordnung durch den Ermittlungsrichter auf Antrag der Staatsanwaltschaft erfolgen, mit einer Eilkompetenz der Staatsanwaltschaft bei Gefahr im Verzug und richterlicher Bestätigung binnen 48 Stunden. Für § 98e StPO-E ist eine ausdrückliche richterliche Anordnung vorzusehen, die den Kreis der einzubeziehenden Datenbestände konkret bezeichnet.

II. Geschlossener Straftatenkatalog für § 98d StPO-E

§ 98d Abs. 1 Nr. 1 StPO-E knüpft die Eingriffsschwelle an eine „Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Absatz 2 bezeichnete Straftat“. Die Formulierung „insbesondere“ macht den Katalogtaten des § 100a Abs. 2 StPO lediglich zu einem Regelbeispielen. Damit erhält die Norm eine Generalklausel, die den Anwendungsbereich weit über die enumerativ aufgezählten Katalogtaten hinaus öffnet.

Dieses Vorgehen widerspricht dem aus dem Rechtsstaatsprinzip (Art. 20 Abs. 3 GG) folgenden Bestimmtheitsgebot und den vom Bundesverfassungsgericht aufgestellten Anforderungen an die gesetzliche Bestimmtheit von Eingriffsbefugnissen (BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19, 1 BvR 2634/20, Rn. 110). Gerade bei Maßnahmen mit hoher Streubreite – der biometrische Abgleich betrifft typischerweise eine Vielzahl unbeteiligter Personen – sollte der Gesetzgeber den Anwendungsbereich durch

einen geschlossenen Katalog präzise eingrenzen. Die vom Entwurf gewählte Formulierung ermöglicht es der Staatsanwaltschaft, den biometrischen Internetabgleich bei nahezu jeder mittelschweren Straftat anzuordnen, sofern sie im Einzelfall als „erheblich“ qualifiziert wird.

Die Generalklausel sollte wenigstens durch einen abschließenden Verweis auf den Straftatenkatalog des § 100a Abs. 2 StPO ersetzt werden. Die Formulierung sollte lauten: „[...] eine in § 100a Absatz 2 bezeichnete Straftat begangen hat [...]“.

III. Kernbereichsschutz und Schutz zeugnisverweigerungsberechtigter Personen

Der Entwurf enthält für keine der beiden Maßnahmen spezifische Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung oder zum Schutz zeugnisverweigerungsberechtigter Personen im Sinne der §§ 53, 53a StPO. Dies ist ein strukturelles Defizit, das sowohl den verfassungsrechtlichen Anforderungen als auch der strafprozessualen Systematik bei vergleichbar eingriffsintensiven Maßnahmen widerspricht.

Für den biometrischen Internetabgleich nach § 98d StPO-E besteht ein spezifisches Risiko der Erhebung kernbereichsrelevanter Daten, da der Abgleich mit im Internet öffentlich zugänglichen biometrischen Daten auch Bilder und Videosequenzen aus intimen oder persönlichkeitsnahen Kontexten erfassen kann. Der pauschale Verweis des Entwurfs auf § 101 StPO genügt nicht, da diese Norm keine Maßstabsregelungen für die spezifischen Risiken biometrischer Abgleichverfahren enthält.

Für die automatisierte Datenanalyse nach § 98e StPO-E ist das Defizit noch gravierender: Durch die verfahrensübergreifende Zusammenführung unterschiedlichster Datenbestände können Profile entstehen, die in den Kernbereich privater Lebensgestaltung hineinreichen, insbesondere wenn Daten aus Telekommunikationsüberwachungen einbezogen werden. Ebenso fehlt eine Regelung, die sicherstellt, dass in der Analyseplattform gespeicherte Daten, die dem Mandatsgeheimnis, dem ärztlichen Geheimnis oder anderen Zeugnisverweigerungsrechten unterliegen, von der automatisierten Verarbeitung ausgenommen werden.

Beide Normen sollten daher um spezifische Kernbereichsschutzregelungen nach dem Vorbild des § 100d Abs. 1-4 StPO und um Regelungen zum Schutz

zeugnisverweigerungsberechtigter Personen nach dem Vorbild des § 160a StPO ergänzt werden.

IV. Biometrische Referenzdatenbanken: Normtextliche Begrenzung und europarechtliche Problematik

§ 98d Abs. 3 StPO-E ordnet zwar die unverzügliche Löschung der beim Abgleich erhobenen und verarbeiteten Daten an, „soweit sie keinen konkreten Ermittlungsansatz für das Verfahren aufweisen." Die Entwurfsbegründung verweist zudem darauf, dass die Erstellung einer dauerhaften biometrischen Referenzdatenbank ausgeschlossen sein soll. Diese zentrale Begrenzung findet jedoch keinen hinreichenden Ausdruck im Normtext selbst.

Der Normtext spricht lediglich von der Löschung der „beim Abgleich erhobenen und verarbeiteten Daten". Es fehlt ein ausdrückliches gesetzliches Verbot der Erstellung und Vorhaltung dauerhafter biometrischer Referenzdatenbanken. Ebenso fehlen normtextliche Vorgaben dafür, dass die für den Abgleich erforderliche Erhebung und Speicherung öffentlich zugänglicher biometrischer Daten ausschließlich anlassbezogen und zeitlich eng begrenzt erfolgen darf.

Europarechtliche Problematik: Art. 5 Abs. 1 lit. e KI-VO

Die europarechtliche Dimension dieses Problems kann nicht überbewertet werden. Art. 5 Abs. 1 lit. e der KI-Verordnung verbietet das Inverkehrbringen, die Inbetriebnahme oder die Verwendung von KI-Systemen, die Datenbanken zur Gesichtserkennung durch das ungezielte Auslesen von Gesichtsbildern aus dem Internet erstellen oder erweitern. Wie das von AlgorithmWatch beauftragte technische Gutachten von Prof. Dr. Lewandowski der Hochschule für Angewandte Wissenschaften Hamburg („Braucht die Polizei eine Datenbank zum biometrischen Abgleich? Das Durchsuchen von Internetbildern zur Gesichtserkennung", September 2025) überzeugend dargelegt und der Wissenschaftliche Dienst des Deutschen Bundestages (Fachbereiche Europa sowie Wirtschaft, Energie und Klima, „Biometrischer Abgleich mit Bildern aus dem Internet, Technische Umsetzung und Vereinbarkeit mit der KI-Verordnung", EU 6 – 074/25 – WD 5 – 105/25, 22. Januar 2026) im Wesentlichen bestätigt hat, lässt sich ein automatisierter biometrischer Abgleich mit

Bildern aus dem Internet technisch nicht ohne die Erstellung einer Referenzdatenbank umsetzen. Die in der Entwurfsbegründung und von der EU-Kommission vertretene Auslegung, wonach das Verbot nur gelte, wenn die Datenbanken mit Hilfe von KI-Systemen erstellt werden, ist eng und rechtsunsicher; sie dürfte Gegenstand gerichtlicher Überprüfung werden.

Unabhängig davon, wie diese Streitfrage letztlich entschieden wird, besteht für den nationalen Gesetzgeber die verfassungsrechtliche Pflicht, die technisch-normativen Grenzen der Datenerhebung und -speicherung im Normtext selbst zu verankern, nicht nur in der Begründung.

In § 98d StPO-E sollten daher folgende normtextliche Begrenzungen aufgenommen werden: (a) ein ausdrückliches Verbot der Erstellung und Vorhaltung dauerhafter biometrischer Referenzdatenbanken als Umsetzungsgebot; (b) eine Begrenzung auf geschlossene, anlassbezogen und zeitlich eng begrenzt erhobene Datensätze; (c) strikte gesetzliche Voraussetzungen für die Nutzung kommerzieller Anbieter (insbesondere hinsichtlich der Herkunft und Zulässigkeit deren Referenzdatenbanken); (d) eine ausdrückliche Kollisionsnorm zu Art. 5 Abs. 1 lit. e KI-VO.

V. Definition der „öffentlich zugänglichen Daten“

Die Entwurfsbegründung definiert „öffentlich zugängliche Daten“ weit. Ausdrücklich sollen auch solche Daten erfasst sein, „die nach vorheriger Registrierung, Genehmigung oder Entgeltzahlung genutzt werden können“. Lediglich Daten, die einer „spezifischen Schwelle unterzogen“ seien, etwa die Einstellung von Daten in sozialen Medien für einen begrenzten Kreis mit Zugangskontrolle, sollen ausgenommen sein.

Diese Definition ist zu weit. Die Einbeziehung registrierungspflichtiger Plattformen – also praktisch aller großen sozialen Netzwerke – in den Kreis der „öffentlich zugänglichen Daten“ erweitert den Anwendungsbereich der Maßnahme erheblich über den vom Entwurf selbst artikulierten Gedanken hinaus, dass die bloße Kenntnisnahme öffentlich zugänglicher Informationen in der Regel keinen Grundrechtseingriff bewirke. Wer Daten auf einer registrierungspflichtigen Plattform einstellt, gibt diese gerade nicht der Öffentlichkeit im strafprozessrechtlichen Sinne preis, sondern hat sich bewusst für einen bestimmten Rahmen entschieden. Das zivilgesellschaftliche Bündnis unter Führung von AlgorithmWatch,

Amnesty International, Chaos Computer Club und der Gesellschaft für Freiheitsrechte (Gemeinsame Presseerklärung vom 15. Oktober 2025) hat zu Recht darauf hingewiesen, dass eine solche Ausweitung faktisch einen flächendeckenden biometrischen Zugriff auf die visuelle Außenseite des digitalen Lebens der Bevölkerung eröffnet.

Die Definition der „öffentlich zugänglichen Daten“ in § 98d StPO-E sollte daher im Normtext enger gefasst werden. Registrierungspflichtige Plattformen sollten grundsätzlich vom Anwendungsbereich ausgenommen werden. Die Norm sollte klarstellen, dass nur solche Daten erfasst sind, die ohne jede Registrierung oder Authentifizierung frei im Internet abrufbar sind.

VI. Gesetzliche Konkretisierung technisch-organisatorischer Sicherungsmaßnahmen

Der Entwurf verweist hinsichtlich der technisch-organisatorischen Sicherungsmaßnahmen überwiegend auf bestehende datenschutzrechtliche Regelungen und auf die KI-Verordnung. Für § 98e Abs. 6 StPO-E beschränkt sich die Regelung auf die generalklauselartige Anordnung, die Einhaltung des geltenden Rechts sei „technisch und organisatorisch sicherzustellen“. § 98e Abs. 4 Satz 5 StPO-E ordnet an, es sei „technisch und organisatorisch sicherzustellen, dass diskriminierende Algorithmen weder herausgebildet noch verwendet werden“.

Derartige Generalklauseln genügen den Anforderungen des Bundesverfassungsgerichts nicht, das in seiner Palantir-Entscheidung (BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19, 1 BvR 2634/20) eine hinreichende gesetzliche Einhegung der Analysemethodik verlangt. Das Gebot normativer Bestimmtheit verlangt, dass der Gesetzgeber die wesentlichen Sicherungsanforderungen nicht allein der Verwaltungspraxis überlässt.

Der Gesetzgeber sollte die folgenden technisch-organisatorischen Anforderungen unmittelbar im Normtext oder in einer gesetzlich vorgeschriebenen Rechtsverordnung regeln: (a) differenzierte Rollen- und Rechtekonzepte mit individuellem Zugriffsschutz; (b) verbindliche Speicherfristen und automatisierte Löschverfahren; (c) revisionssichere Audit-Protokollierung sämtlicher Zugriffe und Abfragen; (d) konkrete Maßstäbe für den Diskriminierungsschutz, einschließlich regelmäßiger Bias-Audits und transparenter Dokumentation der eingesetzten Algorithmen; (e) Vorgaben zur Verwendungsregelung bei der

Zusammenführung von Datenbeständen unterschiedlicher Erhebungszwecke.

VII. Normative Begrenzung der Analysemethodik bei § 98e StPO-E

§ 98e Abs. 4 StPO-E beschreibt die zulässigen Analysemethoden in fünf Nummern. Abs. 4 Satz 1 Nr. 5 lässt die „statistische Auswertung“ gespeicherter Daten zu. In Verbindung mit der grundsätzlichen Zulässigkeit des KI-Einsatzes (Entwurfsbegründung S. 19) eröffnet diese Formulierung einen weiten Raum für den Einsatz lernender Systeme, der durch die in den Sätzen 2 bis 5 vorgesehenen Begrenzungen nicht hinreichend eingegrenzt wird.

Das Bundesverfassungsgericht hat in der Palantir-Entscheidung (BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19, 1 BvR 2634/20, Rn. 146) klargestellt, dass das Eingriffsgewicht umso höher ist, je offener die Methode des Suchvorgangs gestaltet ist, und dass maschinelle Sachverhaltsbewertungen eingriffserhöhend wirken. Vor diesem Hintergrund bedarf es ausdrücklicher normativer Begrenzungen, die bestimmte Formen des KI-Einsatzes ausschließen.

In § 98e Abs. 4 StPO-E sollten daher folgende Ausschlüsse normtextlich verankert werden: (a) Ausschluss prognostischer Scoring-Funktionen, die Personen anhand von Risikobewertungen kategorisieren; (b) Ausschluss automatisierter Priorisierungen mit normativem Gewicht, die über die bloße Sortierung von Trefferlisten hinausgehen; (c) Ausschluss selbstlernender Modelle ohne transparentes Änderungsmanagement, bei denen die Entscheidungslogik nicht nachvollziehbar dokumentiert ist; (d) ausdrückliche Klarstellung, dass der Einsatz generativer KI zur Erzeugung synthetischer Ermittlungsansätze oder hypothetischer Tatszenarien unzulässig ist.

VIII. Eigenständige Zufallsfundregelung für § 98d StPO-E

Der Entwurf enthält für § 98d StPO-E keine eigenständige Zufallsfundregelung. § 98d Abs. 3 StPO-E beschränkt sich darauf, die Löschung der beim Abgleich erhobenen Daten anzuordnen, „soweit sie keinen konkreten Ermittlungsansatz für das Verfahren aufweisen“. Dieser verfahrensbezogene Löschmaßstab lässt in seiner derzeitigen Fassung eine fortdauernde Speicherung strukturell zu bzw. schließt diese nicht ausdrücklich aus.

Der biometrische Internetabgleich zeichnet sich gerade dadurch aus, dass er mit hoher Wahrscheinlichkeit Treffer zu Personen erzielen wird, die weder Beschuldigte noch Ziel des Abgleichs sind. Die Norm regelt nicht, unter welchen qualifizierten Voraussetzungen derartige Zufallsfunde verwertet werden dürfen. Diese Lücke wiegt besonders schwer in umfangreichen Wirtschaftsstrafverfahren mit einer Vielzahl von Beteiligten, in denen der Begriff des „konkreten Ermittlungsansatzes für das Verfahren“ weit ausgelegt werden kann und eine weitreichende Speicherung und Verwertung von Daten gegen Personen ermöglicht, die zum Zeitpunkt der Maßnahme weder beschuldigt noch Ziel des Abgleichs waren.

Wenn der Entwurf selbst die Eingriffsintensität des biometrischen Abgleichs auf dem Niveau der §§ 100g, 100i StPO verortet, muss konsequenterweise auch die Verwertbarkeit von Zufallsfunden entsprechenden qualifizierten Anforderungen unterliegen.

Für § 98d StPO-E sollte eine eigenständige Zufallsfundregelung nach dem Vorbild des § 100e Abs. 6 StPO geschaffen werden. Die Verwertung von Erkenntnissen, die sich beim biometrischen Abgleich gegen bislang nicht beschuldigte Personen oder hinsichtlich anderer Straftaten ergeben, ist an das Vorliegen einer Katalogtat zu knüpfen. Der verfahrensbezogene Löschmaßstab des § 98d Abs. 3 StPO-E ist entsprechend zu präzisieren.

IX. Weitere Regelungsdefizite

1. Fehlende Befristung und Evaluierung

Der Entwurf sieht weder eine Befristung noch eine gesetzliche Evaluierungspflicht vor (Begründung A. VIII.). Die pauschale Begründung, die Regelungen beträfen den „Kernbereich des Strafverfahrensrechts“, überzeugt nicht. Angesichts der Neuartigkeit der Ermittlungsmaßnahmen, der technologischen Dynamik und der erheblichen Grundrechtsbetroffenheit ist eine gesetzliche Evaluierungspflicht nach spätestens fünf Jahren vorzusehen. Vergleichbare landesrechtliche Regelungen im Bereich der Gefahrenabwehr sehen regelmäßig Evaluierungspflichten vor. Die weitere Begründung, wonach die mit dem Gesetz eingeführten neuen Ermächtigungsgrundlagen „grundsätzlich einer fortlaufenden Beobachtung unterzogen“ würden, ist ebenfalls nicht nachzuvollziehen – eine solche Beobachtung durch den Gesetzgeber ist nicht gegeben.

2. Transparenz und Statistikpflichten
Der Entwurf sieht keine jährliche Berichtspflicht der Bundesregierung gegenüber dem Bundestag vor, wie sie etwa in § 100b Abs. 6 StPO für die Online-Durchsuchung vorgesehen ist. Eine solche Berichtspflicht ist im Lichte des Demokratieprinzips und der parlamentarischen Kontrollfunktion unverzichtbar.

3. Anordnungsregelung für § 98e StPO-E
Das vollständige Fehlen einer Anordnungsregelung für § 98e StPO-E stellt ein schwerwiegendes Regelungsdefizit dar. § 98e Abs. 5 StPO-E sieht lediglich eine Begründungs- und Protokollierungspflicht vor, regelt aber weder die Anordnungskompetenz noch die Anordnungsvoraussetzungen in prozeduraler Hinsicht. Dies genügt den rechtsstaatlichen Anforderungen an die Normenklarheit nicht.

4. Zweckbeschränkung des biometrischen Abgleichs auf Personenfahndung und -identifizierung
Der Entwurf beschränkt den Einsatzzweck des biometrischen Internetabgleichs nach § 98d StPO-E nicht auf die Personenfahndung und -identifizierung, sondern lässt diesen auch „zur Erforschung des Sachverhalts“ zu. Damit geht der Entwurf weit über den Anlass hinaus, der die gesetzgeberische Debatte ausgelöst hat – die Identifizierung der gesuchten mutmaßlichen Ex-RAF-Täterin Daniela Klette mittels kommerzieller Biometrie-Software.

Die offene Zweckformulierung legitimiert faktisch sämtliche Recherchemaßnahmen, die in ihrer Gesamtheit die Erstellung eines umfassenden Bewegungs- und Persönlichkeitsprofils der Betroffenen bis hin in ihre höchstpersönlichen Beziehungen und Lebensbereiche zulassen. Viele Menschen bilden ihren persönlichen Lebensbereich umfassend in sozialen Medien ab. Die automatisierte Auswertung dieser Inhalte mittels biometrischer Analysen ermöglicht eine vollständige retrograde Offenlegung höchstpersönlicher privater Beziehungen, Kontakte, Orte, Handlungen, Gewohnheiten und Persönlichkeitsausprägungen. Während Betroffene durch Anonymisierung ihrer Namensidentität einen gewissen Schutz ihrer Persönlichkeit bewirken können, ist dies bei Bildmaterial naturgemäß unmöglich. Ein solch umfassender automatisierter Analysezugriff lässt sich vom Ansatz her bereits nicht mit geltendem Verfassungsrecht vereinbaren.

Die Einsatzmöglichkeiten des biometrischen Abgleichs nach § 98d StPO-E sollten daher auf Zwecke der Personenfahndung und -identifizierung beschränkt werden. Die Formulierung in § 98d Abs. 1 StPO-E sollte entsprechend lauten: „[…] zum Zwecke der Identifizierung oder Aufenthaltsermittlung im Rahmen bereits bestehender Ermittlungsverfahren […]“.

5. Unionsrechtliche Erforderlichkeitsschwelle (Art. 10 RL (EU) 2016/680)

Der Entwurf sieht für den biometrischen Internetabgleich nach § 98d Abs. 1 StPO-E als Subsidiaritätsvoraussetzung vor, dass die Ermittlung oder Identifizierung „auf andere Weise wesentlich erschwert oder aussichtslos wäre“. Diese Formulierung genügt den unionsrechtlichen Anforderungen nicht.

Art. 10 der Richtlinie (EU) 2016/680 (JI-Richtlinie) gestattet die Verarbeitung besonderer Kategorien personenbezogener Daten – wozu biometrische Daten zur eindeutigen Identifizierung gehören – nur, wenn sie „unbedingt erforderlich“ ist. Dieser Maßstab wird durch § 48 Abs. 1 BDSG in das nationale Recht umgesetzt. Die „unbedingte Erforderlichkeit“ im Sinne der JI-Richtlinie stellt eine verschärfte conditio-sine-qua-non dar: Es muss sicher ausgeschlossen sein, dass der angestrebte Erkenntnisgewinn auf andere Weise erlangt werden kann. Die vom Entwurf gewählte Formulierung „wesentlich erschwert“ bleibt hinter diesem Maßstab deutlich zurück, da sie die Maßnahme bereits dann zulässt, wenn alternative Ermittlungswege lediglich aufwändiger, aber nicht ausgeschlossen wären.

Die Subsidiaritätsklausel in § 98d Abs. 1 StPO-E sollte daher an den unionsrechtlichen Maßstab angepasst und wie folgt formuliert werden: „[…] wenn die Identifizierung oder Aufenthaltsermittlung ohne den Abgleich nicht erreicht werden kann“. Damit wird sichergestellt, dass der biometrische Internetabgleich als ultima ratio nur dann eingesetzt werden darf, wenn konventionelle Ermittlungsmaßnahmen nachweislich ausgeschöpft sind oder von vornherein keinen Erkenntnisgewinn versprechen.

6. Auffindeverdacht bei verfahrensübergreifender Datenanalyse nach § 98e StPO-E

§ 98e StPO-E erlaubt die verfahrensübergreifende Zusammenführung und automatisierte Analyse heterogener Datenbestände, ohne für die einzelnen einzubeziehenden

Datenquellen einen konkreten Auffindeverdacht vorauszusetzen. Dies widerspricht der Rechtsprechung des Bundesverfassungsgerichts zur Durchsicht elektronischer Beweismittel.

Das Bundesverfassungsgericht hat in seiner Grundsatzentscheidung zur Durchsuchung elektronischer Datenträger (BVerfG, Beschluss vom 12. April 2005 – 2 BvR 1027/02) nachdrücklich darauf hingewiesen, dass angesichts des mit der Durchsicht elektronischer Beweismittel verbundenen Eingriffs in das Grundrecht auf informationelle Selbstbestimmung eine strenge Beachtung des Verhältnismäßigkeitsgrundsatzes und des Übermaßverbots zu gewährleisten ist. Dies beinhaltet insbesondere, dass vor Beginn einer Durchsicht ein Auffindeverdacht bestehen muss – die konkrete Annahme, dass sich in den zu durchsuchenden Daten verfahrensrelevante Informationen befinden. In der Entscheidung (BVerfG, Beschluss vom 12. April 2005 – 2 BvR 1027/02, Rn. 114) wurde zudem betont, dass bereits bei der Durchsicht zu berücksichtigen ist, dass die Gewinnung überschießender und vertraulicher, für das Verfahren aber bedeutungsloser Informationen im Rahmen des Vertretbaren vermieden werden muss. Eine Durchsicht elektronischer Beweismittel ohne jeden konkreten Auffindeverdacht verbietet sich nach diesen Grundsätzen von vornherein.

Diese Grundsätze sind auf die automatisierte Datenanalyse nach § 98e StPO-E zu übertragen und dort wegen der verfahrensübergreifenden Zusammenführung sogar in verschärfter Form zu beachten. Die Einbeziehung eines Datenbestandes in die Analyseplattform kommt funktional einer Durchsicht gleich; durch die automatisierte Verarbeitung wird die Eingriffsintensität zusätzlich gesteigert. Gerade in umfangreichen Wirtschaftsstrafverfahren mit einer Vielzahl von Beteiligten und komplexen Datenbeständen besteht die Gefahr, dass ohne ein qualifiziertes Auffindeverdacht-Erfordernis eine weitgehend anlasslose Durchsuchung sämtlicher verfügbarer Daten stattfindet.

§ 98e StPO-E sollte daher um eine ausdrückliche Regelung ergänzt werden, wonach für jede in die Analyse einzubeziehende Datenquelle vor dem Analysevorgang geprüft und dokumentiert werden muss, warum hinsichtlich des konkret einbezogenen Datenbestandes ein Auffindeverdacht besteht und warum eine Verwertung der darin möglicherweise enthaltenen Erkenntnisse überhaupt in Betracht kommt. Die einzubeziehenden Datenquellen sind in der richterlichen Anordnung konkret zu bezeichnen und zu begrenzen.

7. Dokumentation und Reproduzierbarkeit des Suchvorgangs

Der Entwurf enthält für beide Maßnahmen keine hinreichenden Dokumentationspflichten, die eine vollständige Reproduzierbarkeit des Suchvorgangs gewährleisten. Dies betrifft sowohl den biometrischen Internetabgleich nach § 98d StPO-E als auch die automatisierte Datenanalyse nach § 98e StPO-E.

Für den biometrischen Abgleich nach § 98d StPO-E ist eine präzise Dokumentation der konkreten Suchanfragen einschließlich des verwendeten Referenzmaterials und der jeweiligen Suchergebnisse – einschließlich der Negativergebnisse – für die Bewertung der Beweiskraft in einer späteren strafprozessualen Hauptverhandlung unabdingbar. Bei Gesichtsidentifikationen sind erhebliche Priming-Effekte bei der nachfolgenden menschlichen Bewertung zu erwarten: Hat ein Ermittlungsbeamter einen KI-generierten Treffer als „Ergebnis“ vor Augen, wird seine nachfolgende eigenständige Identifizierungsentscheidung durch dieses Ergebnis systematisch beeinflusst. Ohne eine vollständige Dokumentation des gesamten Suchvorgangs einschließlich sämtlicher unergiebiger Anfragen und verworfener Treffer sind weder Gericht noch Verteidigung in der Hauptverhandlung in der Lage, die Verlässlichkeit und Beweiskraft des biometrischen Identifizierungsergebnisses sachgerecht zu überprüfen.

Gleiches gilt für die automatisierte Datenanalyse nach § 98e StPO-E. § 98e Abs. 5 StPO-E sieht zwar eine Begründungs- und Protokollierungspflicht vor; diese wird aber nicht hinreichend spezifiziert, so dass offen bleibt, welche konkreten Umstände zu protokollieren sind.

Für beide Maßnahmen sollte daher eine gesetzliche Pflicht zur Schaffung einer Datenlage normiert werden, die eine vollständige Reproduktion des gesamten Such- und Analysevorgangs ermöglicht. Dies umfasst insbesondere: (a) die vollständige Protokollierung sämtlicher Suchanfragen einschließlich des verwendeten Referenzmaterials und der Suchparameter; (b) die Dokumentation aller erzielten Treffer und Zwischenergebnisse, einschließlich verworfener und unergiebiger Ergebnisse; (c) die Dokumentation der angewandten Algorithmen und ihrer Versionen; (d) die Sicherstellung, dass diese Dokumentation der Verteidigung im Rahmen der Akteneinsicht nach § 147 StPO vollständig zugänglich gemacht wird.

X. Gesamtbewertung und Fazit

Die Schaffung gesetzlicher Grundlagen für den Einsatz digitaler Ermittlungsinstrumente ist verfassungsrechtlich geboten und kriminalpolitisch begrüßenswert. Die Palantir-Entscheidung des Bundesverfassungsgerichts (BVerfG, Urteil vom 16. Februar 2023 – 1 BvR 1547/19, 1 BvR 2634/20) und die KI-Verordnung der EU schaffen insoweit einen klaren Handlungsauftrag für den Gesetzgeber.

Der vorliegende Referentenentwurf wird diesem Auftrag in seiner derzeitigen Fassung jedoch nicht gerecht. Er weist erhebliche strukturelle Defizite auf, die im Kern darin bestehen, dass die Maßnahmen nicht mit den rechtsstaatlichen Sicherungen versehen werden, die ihre Eingriffsintensität erfordert. Die Einstufung der Eingriffsintensität auf dem Niveau der §§ 100g, 100i StPO durch den Entwurf selbst bildet den tatsächlichen Eingriffsgehalt nicht hinreichend ab.

Insbesondere die Frage der europarechtlichen Vereinbarkeit des biometrischen Internetabgleichs mit Art. 5 Abs. 1 lit. e KI-VO ist durch den Entwurf nicht überzeugend gelöst. Die Argumentation, das Verbot gelte nur bei Einsatz von KI-Systemen zur Datenbankerstellung, ist eng und trägt dem Schutzzweck der Norm nicht hinreichend Rechnung. Es besteht das erhebliche Risiko, dass ein auf dieser Grundlage ergangenes Gesetz vor dem EuGH oder dem Bundesverfassungsgericht keinen Bestand haben wird.

Es wird daher empfohlen, den Entwurf unter Berücksichtigung der vorstehenden Kritikpunkte grundlegend zu überarbeiten. Die Erweiterung der strafprozessualen Eingriffsbefugnisse um digitale Ermittlungsmaßnahmen ist nur dann verfassungsrechtlich tragfähig und rechtsstaatlich nachhaltig, wenn sie von wirksamen rechtlichen Sicherungen flankiert wird.

****