Stellungnahme der Strafverteidigervereinigungen

zum Referent:innenentwurf des BMJV zur Änderung der Strafprozessordnung – digitale Ermittlungsmaßnahmen

Berichterstatter:innen:

Clemens Hof (Berlin)
Dr. Sonia Krogmann (Berlin)
Dr. Benedikt Mick (Berlin)
Nina Wittrowski (Berlin)

Berlin, 6. April 2026

VORBEMERKUNG

Der vom Bundesministerium der Justiz und für Verbraucherschutz am 12. März 2026 zur Stellungnahme übersandte Referentenentwurf zur Änderung der Strafprozessordnung – digitale Ermittlungsmaßnahmen knüpft an eine Reihe gesetzgeberischer Änderungen der Strafprozessordnung in den letzten Jahren an (zuletzt weitreichend im Jahr 2021 mit dem Gesetz zur Fortentwicklung der Strafprozessordnung BT-Drucks. 19/27654 = BGBl. 2021 S. 2099), die eine stete Ausweitung der Befugnisse von Ermittlungsbehörden zum Inhalt haben.

Auch dieser Referentenentwurf verfolgt das Ziel, Strafverfolgungsbehörden mit neuen Befugnissen auszustatten, um die Effektivität der Strafverfolgung zu steigern.

Die Strafverteidigervereinigungen sehen das Erfordernis, die Befugnisse der Ermittlungsbehörden an die technischen Fortschritte anzupassen. Gleichwohl halten die Vereinigungen den Gesetzesentwurf für zu weitreichend. Insbesondere trägt der Entwurf den technischen Gefahren und Unsicherheiten zu wenig Rechnung. Er begegnet in mehrfacher Hinsicht verfassungsrechtlichen, unionsrechtlichen und rechtspolitischen Bedenken.

GEGENSTAND UND ZIEL DES ENTWURFS

Der vorliegende Referentenentwurf verfolgt das erklärte Ziel, Strafverfolgungsbehörden mit neuen Befugnissen auszustatten, um die Effektivität der Strafverfolgung zu steigern. Zu diesem Zweck sollen zwei neue Ermächtigungsgrundlagen in die Strafprozessordnung eingefügt werden:

- § 98d StPO-E: Ermächtigung zum automatisierten biometrischen Abgleich von Daten aus einem Strafverfahren mit im Internet öffentlich zugänglichen biometrischen Daten.
- § 98e StPO-E: Ermächtigung zur automatisierten verfahrensübergreifenden Datenanalyse mittels polizeilicher Recherche- und Analyseplattformen.

Diese beiden Ermächtigungsgrundlagen sollen den Ermittlungsbehörden ermöglichen, biometrische Daten aus einem Strafverfahren mit im Internet öffentlich zugänglichen Daten automatisiert abzugleichen. Derzeit ist ein solcher Abgleich nur manuell, also ohne den Einsatz einer speziellen für den Abgleich entwickelten Software, unter Einsatz gängiger Internet-Suchmaschinen zulässig, um Personen zu identifizieren, zu lokalisieren oder Tat-Täter-Zusammenhänge zu erschließen. Zugleich sollen die Ermittlungsbehörden die Befugnis erhalten, 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.

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 – so steht es im Referentenentwurf.

KRITIK

I. § 98d StPO-E: Automatisierter biometrischer Abgleich mit öffentlich zugänglichen Daten aus dem Internet

Wie oben bereits ausgeführt, soll mit dem § 98d StPO-E eine Ermächtigungsgrundlage geschaffen werden für den automatisierten Abgleich von biometrischen Daten aus einem Strafverfahren mit solchen, die öffentlich zugänglich sind. Bisher ist ein solcher Abgleich biometrischer Daten nur manuell, also ohne den Einsatz einer speziellen, für den Abgleich entwickelten Software zulässig (sog. OSINT-Maßnahme). Durch § 98d StPO-E soll nunmehr die Nutzung von KI-basierter Gesichtserkennungssoftware – ähnlich der zu PimEyes oder ClearView-AI – ermöglichen.

Im Jahr 2024 hat es bereits einen Entwurf zu § 98d StPO gegeben, der die Rechtsgrundlage für einen KI-basierten biometrischen Abgleich sein sollte.[1] Der damalige Entwurf war, im Vergleich zum jetzt vorliegenden, noch deutlich enger gefasst. So sollte der Einsatz einer entsprechenden KI nur zulässig sein bei einem qualifizierten Tatverdacht hinsichtlich einer der Katalogtaten des § 100b StPO und der Entwurf sah grundsätzlich einen Richtervorbehalt vor.[2] Diese beiden Voraussetzungen sollten aus Sicht der Strafverteidigervereinigungen auch in den jetzigen Entwurf aufgenommen werden.

Der § 98d StPO-E bedeutet einen Eingriff in das verfassungsrechtlich verbürgte Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG). Das BVerfG hat festgestellt:

> »Die freie Entfaltung der Persönlichkeit unter den modernen Bedingungen der Datenverarbeitung (setz) den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus«.[3]

Das Recht auf informationelle Selbstbestimmung gewährleistet daher die Befugnis jedes Einzelnen selbst darüber zu bestimmen, welche persönlichen Daten preisgegeben und verwendet werden.[4] Staatliche Überwachungs- und Ermittlungsbefugnisse sind gerade auch im Bereich der Strafverfolgung rechtfertigungsbedürftig und ihre Verfassungsmäßigkeit hängt von den sich aus den betroffenen Grundrechten jeweils ergebenden Grenzen und Verhältnismäßigkeitsanforderungen ab.[5] Dabei ist im Rahmen der gebotenen Abwägung und Verhältnismäßigkeitsprüfung insbesondere einzustellen, ob es sich um Bestimmung mit einer großen Streubreite handelt.[6] Durch den § 98d StPO-E ist das Recht auf informationelle Selbstbestimmung unfraglich betroffen, weil persönliche Daten – auch wenn öffentlich zugänglich – für Ermittlungsmaßnahmen verwendet werden. Es handelt sich auch um eine Bestimmung, die eine große Streubreite aufweist, weil es mittels einer Gesichtserkennungssoftware möglich wäre, Millionen Bilder aus dem Internet zum Abgleich heranzuziehen und zu benutzen und entsprechend viele Personen betroffen sind, deren Gesichter in den Abgleichsbildern enthalten sind. Die Eingriffsintensität wird durch den § 98d StPO-E zudem durch die Faktoren der Richtigkeitswahrscheinlichkeit und der Nachvollziehbarkeit des eingesetzten Programms erhöht (dazu sogleich ausführlich unter 3.).[7] Besonders problematisch ist es aus Sicht der Strafverteidigervereinigungen, dass der Einsatzzweck des § 98d StPO-E nicht auf Identitätsfeststellung oder die Aufenthaltsermittlung eines Beschuldigten beschränkt ist, sondern generell »zur Erforschung des Sachverhalts« dienen kann. Dies birgt letztlich die Gefahr, dass Bewegungs- und Persönlichkeitsprofile von Beschuldigten erstellt werden können. Ein solch weitreichender Eingriff kann – obwohl der Abgleich nur mit ohnehin öffentlich zugänglichen Daten erfolgen darf – auch in den Bereich höchstpersönlicher Lebensgestaltung hineinreichen.

Vor dem Hintergrund des eben dargelegten Eingriffs in die Grundrechte der Betroffenen, ist die Eingriffsschwelle für den § 98d StPO-E zu niedrig angesetzt. Ein Richtervorbehalt kann wegen der generellen Bedenken mit Blick auf dessen Wirksamkeit

1 BT-Drs. 20/13413, S. 38 ff.

2 BT-Drs. 20/13413, S. 38.

3 BVerfG, NJOZ 2021, 1391, 1393 f.(Rn. 198)

4 BVerfG aaO.

5 BVerfG, NJOZ 2021, 1391, 1394 (Rd. 200).

6 BVerfG, NJOZ 2021, 1391, 1394 (Rd. 202).

7 So auch *Rückert*, StV 2025, 350, 351.

zum Schutz der Rechte von Betroffenen nur eine absolute Mindestvoraussetzung darstellen. Der Entwurf sieht nach Absatz 4 die Anordnungskompetenz grundsätzlich bei der Staatsanwaltschaft. Bei »Gefahr im Verzug« kann ein entsprechender Abgleich auch durch Ermittlungspersonen der Staatsanwaltschaft erfolgen. Insoweit weisen die Strafverteidigervereinigungen auf den problematischen Umgang mit der Anordnung bei Gefahr im Verzug und der Bejahung entsprechender Umstände hin, die sich bereits jetzt in Bezug auf andere Normen zeigen.

Der Entwurf belässt somit in bedenklicher Weise die Anordnung des biometrischen Internetabgleichs bei der Staatsanwaltschaft und sieht nur bei Eilmaßnahmen eine binnen 48 Stunden nachzuholende Entscheidung vor; unionsrechtlich verlangt Art. 26 Abs. 10 KI-VO jedoch eine bindende, justiziell überprüfbare Entscheidung einer Justiz- oder Verwaltungsbehörde, was aus rechtsstaatlichen Gründen durch einen ausdrücklichen Richtervorbehalt flankiert werden sollte.

Unabhängig von den bisher aufgezeigten rechtlichen Problemen im Hinblick auf den fehlenden Richtervorbehalt und den Verstoß gegen Verfassungsrecht, stellt sich nicht zuletzt die Frage, ob und wie der Entwurf technisch und rechtlich umgesetzt werden kann.

Bei dem Einsatz einer Gesichtserkennungs-KI, handelt es sich nach Art. 6 Abs. 2 der KI-Verordnung i.V.m. Anhang III Nr. 1a um ein sog. Hochrisiko-KI-System. Hinzukommt, dass Art. 5 Abs. 1 e KI-VO den Aufbau von Gesichtserkennungsdatenbanken durch ungezielte Auslese von Gesichtsbildern aus dem Internet verbietet. Auf genau einer solchen Sammlung von gespeicherten Bildern, die öffentlich zugänglich sind, beruhen aber Systeme wie ›PimEyes‹. Die von Ermittlungsbehörden eingesetzte KI müsste für einen entsprechenden Abgleich zunächst alle öffentlich im Netz verfügbaren Bilder von Gesichtern durchsuchen, sammeln und in Templates umrechnen.[8] Bei der Speicherung der Templates entstehen jedoch zwangsläufig Datenbanken.

Der Gesetzesentwurf sieht bisher auch keine Pflicht vor, diese Vergleichsdatenbanken zu löschen. In § 98d Abs. 3 ist lediglich normiert, dass die beim Abgleich erhobenen und verarbeiteten Daten nach Durchführung unverzüglich zu löschen sind, soweit sie keinen Ermittlungsansatz für das Verfahren aufweisen. Eine Löschpflicht in Bezug auf die Vergleichsdatenbanken – die für eine Vereinbarkeit mit der KI-VO indes Voraussetzung ist – muss in die gesetzliche Regelung aufgenommen werden. Die Strafverteidigervereinigungen sehen zudem die Gefahr, dass ohne ein entsprechendes ausdrückliches Verbot, Datenbanken letztlich unter Umgehung des Art. 5 Abs. 1 e KI-VO erstellt werden. Im Gesetzesentwurf heißt es nämlich, das Verbot aus Art. 5 Abs. 1 e KI-VO gelte nicht, »sofern für das Auslesen der Daten keine KI-Systeme eingesetzt werden« (S. 11). Konkret bedeutet das, so lange eine Vergleichsdatenbank nicht mit Hilfe einer KI erstellt wurde, also die Abspeicherung der öffentlich zugänglichen Bilder beispielsweise manuell erfolgen, soll die Erstellung einer Vergleichsdatenbank zulässig sein. Damit liefe die Regelung des Art. 5 Abs. 1 e KI-VO – und ihr Schutzbereich – aber praktisch leer, weil es dann alleine auf den Zeitpunkt ankäme, zu dem die KI eingesetzt würde (nämlich erst nachdem Bilder anders als durch eine KI abgespeichert sind) und eröffnete der Willkür das Tor. Eine sinnvolle technische Umsetzung des § 98d StPO-E ist daher ohne Erstellung einer eigenen Datenbank und -sammlung – und aus Sicht der Strafverteidigervereimnigungen damit unter Verstoß gegen die KI-VO – technisch gar nicht umsetzbar. Die Einhaltung der KI-VO ist jedoch zwingend erforderlich, um das Gefühl einer jederzeitigen Überwachung und damit

8 So Leisegang und Köver in ihrem Artikel »Bundesregierung will biometrische Fotofahndung im Netz«: https://netzpolitik.org/2026/rechtlich-fragwuerdig-bundesregierung-will-biometrische-fotofahndung-im-netz/; zuletzt abgerufen am 26. März 2026

einhergehende sog. ›Chilling Effects‹, also die Gefahr des Verzichts der Ausübung der eignen Grundrechte, zu vermeiden

Die Norm enthält zwar eine Löschpflicht für »beim Abgleich erhobene und verarbeitete Daten« und stellt in der Begründung klar, dass dies auch Templates umfassen sowie die Einrichtung einer dauerhaften Referenzdatenbank ausschließen soll; normenklar ist dies im Gesetzestext aber nicht hinreichend abgesichert, sodass eine explizite Verbots- und Löschregel für Referenzdatenbanken (einschließlich temporärer Template-Sammlungen) aufzunehmen ist, um Umgehungen des Verbots des Art. 5 Abs. 1 Buchst. e KI-VO effektiv zu verhindern. Die ministerielle Lesart, das unionsrechtliche Verbot gelte nur, wenn das Auslesen selbst per KI erfolge, würde in der Praxis das anlasslose Scraping lediglich in ein vorgelagertes »non-KI«-Stadium verlagern; zivilgesellschaftliche und wissenschaftliche Stimmen warnen aber, dass ohne tragfähige Referenzdatenbank ein sinnvoller Abgleich nicht möglich ist und das Vorhaben damit rechtlich wie praktisch scheitert – was einer klaren gesetzlichen Untersagung ex ante bedarf.

Aus Verteidiger:innensicht sind zwei weitere Aspekte problematisch: Zum einen die fehlende Überprüfbarkeit der auf Grundlage des § 98d StPO-E generierten Daten. Das betrifft vor allem die Richtigkeitswahrscheinlichkeit und die Nachvollziehbarkeit des eingesetzten Programms. Denn eine entsprechende Nachvollziehbarkeit der eingesetzten Systeme setzt voraus, dass die Zuverlässigkeit der eingesetzten Programme sich wissenschaftlich nachvollziehen lässt (sog. ›White-Box‹-KI).[9] Dazu wiederum müssten Erkenntnisse vorliegen, wie eine Gesichtserkennungs-KI arbeitet und vor allem auf welcher Grundlage sie trainiert und fortgebildet wird. Dies ist allerdings technisch nicht möglich, weil teilweise die Ersteller der KI-Softwares selbst nicht klar erklären können, auf welcher Grundlage die KI lernt. Diese ›Black-Box‹-KI entspricht vielmehr dem heutigen Standard. Dieser Standard hat sich aber letztlich ohne Rücksicht auf Rechtsfragen entwickelt. Denn die Software Anbieter blenden, einer wohl generellen Einstellung des ›Silicon Valley‹ enstprechend, solche Fragen regelmäßig aus. Die damit einhergehenden Folgen zeigen sich dann oft später, und sind für die Gesellschaften nicht selten erheblich. Vor allem aber können die Folgen regelmäßig nicht oder nur noch schlecht repariert werden. Nicht zuletzt hängt die Trefferquote und – viel entscheidender – die falsch-positiv Quote davon ab, auf welcher Grundlage die KI trainiert und lernt. All das sind jedoch Fragen, die nach dem aktuellen Stand der Wissenschaft nicht beantwortet werden können.

Beschuldigte haben ein Recht auf möglichst frühzeitigen und umfassenden Zugang zu Beweismitteln und Ermittlungsvorgängen und auf die Vermittlung der erforderlichen materiell- und prozessrechtlichen Informationen, ohne die sie ihre Rechte nicht wirkungsvoll wahrnehmen können. Übertragen auf das Strafverfahren würde der Einsatz einer Gesichtserkennungs-KI bedeuten, dass es für die Verteidigung und die Angeklagten quasi unmöglich wäre herauszubekommen, wie und auf welcher Grundlage die Daten von der Gesichtserkennungs-KI generiert wurden und ob diese möglicherweise manipuliert worden sind. Das beinhaltet die Gefahr, dass Angeklagte gleichsam zum Objekt des Strafverfahrens werden, weil die übermächtigen staatlichen Ermittlungsbefugnisse nicht mehr nachvollziehbar und auch nicht überprüfbar sind.

Der Entwurf schafft ein gravierendes strukturelles Informationsgefälle: Die Ermittlungsbehörden verfügen über das vollständige Ergebnis des biometrischen Abgleichs und der verfahrensübergreifenden Datenanalyse, während die Verteidigung weder

9 So auch *Rückert*, StV 2025, 350, 356.

Kenntnis von den eingesetzten Systemen noch von deren Fehlerquoten, Trainingsgrundlagen oder Algorithmen erlangen kann. Dies würde einen erheblichen Verstoß gegen das Prinzip der Waffengleichheit und das Recht auf ein faires Verfahren bedeuten. Im Kontext automatisierter Ermittlungsmaßnahmen bedeutet dies: Protokolldaten, Systemdokumentationen, Testberichte und Validierungsunterlagen des eingesetzten KI-Systems müssen der Verteidigung zugänglich sein. Der Entwurf sieht lediglich eine Protokollierungspflicht vor, die nur den Namen der Software, den Zeitpunkt des Einsatzes und die durchführende Organisationseinheit erfasst. Dies genügt für eine effektive Verteidigung bei weitem nicht.

Das Bundesverfassungsgericht hat in seiner ANOM-Entscheidung[10] betont, dass Erkenntnisdefizite hinsichtlich der Erhebungsmethode den Rechtsschutz im Hauptverfahren strukturell einschränken und ein Verwertungsverbot gebieten können: Denn das Tatgericht hat – jedenfalls nach einem Verwertungswiderspruch – zu prüfen, ob der Verwertung eines Beweismittels Verwertungsverbote entgegenstehen, was nicht geprüft werden kann, wenn über das Beweiserhebungsverfahren nichts bekannt ist. Eine Protokollierung, die nur den Namen einer Software nennt, nicht aber deren Fehlerquoten, Trainingsdaten und Validierungsergebnisse, ermöglicht keine sachkundige Überprüfung des Ergebnisses. Insoweit sollten mindestens die Ermittlungsbehörden dazu angehalten werden, den Einsatz von Gesichtserkennungssoftware weitreichend zu dokumentieren, um eine spätere Überprüfung der Treffer durch die Verteidigung und die Justiz nachvollziehbar zu machen. Nur eine derartige Dokumenation entspricht einem Staat, der sein Handeln nachvollziehbar macht, also einem Rechtsstaat. Die IT-Industrie hingegen operiert bei diesen Fragen – durchaus bewusst – obskur. Sie verfolgt damit eigene Interessen im Wettbewerb mit der dieser Industrie eigenen Tendenz zur Erlangung von Monopolen. Derartige Interessen haben aber im Strafverfahren nichts verloren: Dort muss der Staat Rechenschaft über seine Ermittlungen ablegen und darf sich nicht hinter obskuren Ermittlungshilfen verstecken.

Für Systeme zur biometrischen Fernidentifizierung sind schließlich unionsrechtlich zusätzliche Sicherungen zwingend: keine ausschließlich automatisierten, nachteiligen Entscheidungen, verpflichtende Einsatzdokumentation und – besonders relevant – eine doppelte menschliche Überprüfung von Identifizierungsergebnissen; diese Garantien sollten als Tatbestandsvoraussetzungen im Gesetzestext verankert werden, nicht bloß in der Begründung.

II. § 98e StPO-E: Ermächtigung zur automatisierten verfahrensübergreifenden Datenanalyse mittels polizeilicher Recherche- und Analyseplattformen

Der Gesetzentwurf zum neu geschaffenen § 98e StPO soll zukünftig die Zusammenführung bisher unverbundener polizeilicher Datei- und Informationssysteme in einer einheitlichen Analyseplattform ermöglichen. Oder anders ausgedrückt: Der § 98e StPO-E würde eine Rechtsgrundlage dafür schaffen, alle personenbezogenen (sensiblen) Daten auf einer einzigen Plattform zu bündeln und auszuwerten.

§ 98e StPO-E verknüpft hochgradig eingriffsintensive Erhebungsresultate aus den §§ 100a ff. StPO mit einer verfahrensübergreifenden Analyseplattform, deren Erkenntnistiefe und Streubreite das Eingriffsgewicht qualitativ erhöht, was einen sorgen muss. Ohne strengere, justiziabel ausgestaltete Eingriffsschwellen, ex ante wirksamer technischer Zweckbindungsarchitektur, klarer methodischer Verbote

10 2 BvR 625/25 vom 23. September 2025

und veröffentlichter Standardisierungen droht eine schleichende Verschärfung des ohnehin schon bedrohlichen Wirkkreises der §§ 100a ff. StPO durch eine noch intensivere »Zweitverarbeitung«, auch mit erheblichen verfassungsrechtlichen Risiken im Lichte der ›Palantir-Entscheidung‹ des BVerfG.[11] § 98e StPO-E weist aufgrund der Breite der Datenquellen und der erlaubten Analyseoperationen ein hohes EigenEingriffsgewicht auf; das BVerfG verlangt für automatisierte Analyseplattformen aber eine strikte Daten- und Methodeneinhegung sowie spezifische gesetzliche Ermächtigungen, da solche Systeme eigenständige Belastungseffekte jenseits der Primärerhebung entfalten.

1. § 98e StPO-E soll Strafverfolgungsbehörden ermächtigen, in polizeilichen Datei- und Informationssystemen rechtmäßig gespeicherte, für eine Analyseplattform zusammengeführte personenbezogene Daten mittels einer automatisierten Anwendung weiterzuverarbeiten, wenn »bestimmte Tatsachen« (sic!) den Verdacht einer auch im Einzelfall schwerwiegenden, in § 100a Abs. 2 StPO bezeichneten schweren Straftat begründen.

Einbezogen werden dürfen u.a. Vorgangs- und Falldaten, Daten aus polizeilichen Informationssystemen sowie Daten aus dem polizeilichen Informationsaustausch; ergänzend – »soweit erforderlich« (sic!) – auch Daten aus Maßnahmen nach §§ 100a, 100f, 100g, 100k Abs. 1 und 2, § 100i StPO und aus Asservaten; Daten aus Online-Durchsuchung und akustischer Wohnraumüberwachung der §§ 100b, 100c StPO sollen (vorerst) ausgeschlossen sein.

Es soll zwar eine direkte Anbindung an nicht-polizeiliche Register und Internetdienste untersagt bleiben; gezielte – auch automatisierte – Einzelabfragen in Registern und Einzelfalldaten aus Internetquellen dürften jedoch einbezogen werden.

2. Das BVerfG hat den Eigen-Eingriffsgehalt automatisierter Analyseplattformen ausdrücklich hervorgehoben: Je weiter Datenarten/-mengen und Methoden reichen, desto eher gelten die strengen Voraussetzungen wie bei heimlichen, eingriffsintensiven Maßnahmen – nämlich der Schutz besonders gewichtiger Rechtsgüter und wenigstens eine konkretisierte Gefahr; unterhalb davon bedarf es enger gesetzlicher Begrenzungen von Daten und Methode, flankiert von Transparenz und wirksamer Kontrolle. Der Entwurf des § 98e bewegt sich – wegen Breite der Datenquellen und Analyseoperationen – in einem hohen Eigengewicht, das deutlich über einen »bloßen maschinellen Abgleich« hinausgeht.

Anzuerkennen ist daher allenfalls, dass der Entwurf zumindest bemüht scheint, einige der Palantir-Kernforderungen – Ausschluss der §§ 100b, 100c-Daten, Verbot der direkten Außenanbindung, anlassbezogene, manuelle Auslösung mit fallkonkreten Suchbegriffen, Verbot ausschließlich automatisierter Entscheidungen, sowie Vorgaben gegen diskriminierende Algorithmen – zu adressieren. Das stärkt gewiss die methodische Einhegung und mindert offene, anlasslose Suchen, könnte sich aber in der Praxis auch schnell als Feigenblatt herausstellen.

Denn die Einbeziehung besonders sensibler Daten aus den Eingriffen gem. §§ 100a, 100f, 100g, 100k, 100i StPO »soweit erforderlich« gerät erkennbar zu weit, kann und wird – kombiniert mit Vorgangs- und Falldaten sowie polizeilichen Informationssystemen – faktisch zu einem breiten, personenbezogenen Datenpool führen. Das BVerfG verlangt aber gerade hier normklare, technisch-organisatorisch gesicherte Zweckbindungs- und Kennzeichnungsvorgaben sowie die vorsorgliche Aussonde-

11 Urt. v. 16.02.2023 - 1 BvR 1547/19 + 2534/20 = BVerfGE 165, 363.

rungssperre für hochsensibles Material; diese müssen vor der Analyse praktisch wirksam sein.

§ 98e StPO-E soll die ergänzende Einbeziehung von Ergebnissen aus TKÜ, Quellen-TKÜ, Standort- und Verkehrsdaten, IMSI-Catcher und Asservaten »soweit erforderlich« ermöglichen. Schon die Erhebung dieser Daten greift aber – teils zeitgleich – in Art. 10 GG und das IT-System-Grundrecht ein (Quellen-TKÜ) und unterliegt daher besonders strengen Verhältnismäßigkeitsanforderungen. Ihre nachträgliche verfahrensübergreifende Verknüpfung in einer Analyseplattform steigert das Eingriffsgewicht zusätzlich, weil sie neue, persönlichkeitsrelevante Erkenntnisse erschließen kann, die dem Einzelnen nicht mehr zurechenbar sind und eine erhebliche Streubreite erzeugen können.

Der Entwurf verweist zwar darauf, dass Verwendungs- und Zweckbindungsregeln fortgelten sollen und technisch-organisatorisch sicherzustellen sind. Verfassungsrechtlich genügt das aber nur, wenn die Einhaltung vor dem Start der Analyseplattform praktisch gesichert ist, damit Daten aus besonders schwerwiegenden Eingriffen nicht faktisch in den allgemeinen Analysepool geraten. Genau hier liegt das Risiko: Ohne zwingende, ex ante wirksame Kennzeichnung und Filterung entsteht zwangsläufig ein ›Sogeffekt‹, der TKÜ-Beifang, Funkzellen-Massenbestände oder sensible Asservate als Rohstoff für sekundäre Profilbildungen nutzbar macht – mit Umgehung der strengen Zweck- und Schwellenlogik der §§ 100a ff. StPO und der verfassungsgerichtlich geforderten Einhegung solcher Datenweiterverwendungen.

Der besondere Schutz des Fernmeldegeheimnisses fungiert als »Sperrriegel« gegen Globalangriffe und verlangt erhöhte Hürden bei Zugriff und Weiterverwendung; dies gilt erst recht, wenn Verkehrsdaten/Funkzellenabfragen massenhaft Unbeteiligte erfassen.[12] Wird solcher Datenbestand in § 98e-Analysen breit verknüpft, droht eine strukturelle Absenkung der Schutzstandards durch »Verarbeitung zweiter Ordnung«. Das widerspricht dem vom BVerfG geforderten abgestuften Schutz je nach Eingriffsgewicht und dem Erfordernis einer gesicherten Tatsachenbasis für Eingriff und Erstreckung auf Dritte.

§ 98e Abs. 4 StPO-E autorisiert das Identifizieren und Herstellen von Beziehungen, Klassifizieren, Struktur-Analysen, Visualisieren und das Gewichtungs-Scoring von Suchkriterien bis hin zur Statistik. Genau diese Schritte sind nach der ›Palantir-Entscheidung‹ des BVerfG[13] besonders eingriffssteigernd, wenn sie offen, mehrstufig und nicht streng an fallkonkrete Suchmuster gebunden erfolgen; maschinelle Sachverhaltsbewertungen (»predictive«-Aussagen) wären zu untersagen. Zwar verbietet § 98e Abs. 4 eine ausschließlich automatisierte, unmittelbar nachteilige Entscheidung und fordert anlassbezogene, manuelle Auslösung sowie fallbezogene Suchbegriffe. Doch damit ist die methodische Einhegung noch nicht abgeschlossen: Es fehlen gesetzliche Klarstellungen zum Ausschluss selbstlernender Systeme, zur Begrenzung von Mehrfachverknüpfungen, zu zulässigen Ergebnisarten und zu standardisierten, veröffentlichten Suchmuster-Leitlinien. Ohne diese Vorgaben bleibt die praktische Schwelle für »offene« Suchen zu niedrig.

3. Die pauschale Zielsetzung, die Effektivität der Strafverfolgung durch automatisierte biometrische Abgleiche und verfahrensübergreifende Analyseplattformen zu ›steigern‹, ist als Rechtfertigung für heimliche, streubreitenstarke Eingriffe

12 BGH Urteil v. 09.01.2025 – 1 StR 54/24

13 s. Fn. 11

unzureichend, weil der verfassungsrechtliche Verhältnismäßigkeitsmaßstab bei datenintensiven Maßnahmen eine Ausrichtung auf den Schutz besonders gewichtiger Rechtsgüter und eine wenigstens konkretisierte Gefahr bzw. qualifizierte Verdachtslage verlangt; generische Effizienzziele riskieren eine Absenkung der Eingriffsschwellen, unterlaufen die Zweckbindung und befördern Einschüchterungseffekte weit über den Kreis der Verdächtigen hinaus.

Ebenso verfehlt das Ziel einer »digitalen Modernisierung« die unions- und verfassungsrechtlichen Leitplanken, wenn es faktisch auf eine weitreichende Vernetzung und Sekundärverwertung bereits hoch eingriffsintensiv erhobener Daten hinausläuft: Für Folgeeingriffe ist das Eingriffsgewicht gerade wegen der Vorbelastung erhöht und erfordert strikte, normklare Zweckbegrenzungen und Schutzmechanismen; zudem schließen unionsrechtliche Vorgaben zur automatisierten Verarbeitung nach dem JIDatenschutzrahmen nachteilige Folgen ohne gesetzliche Garantien aus und verlangen eine strikte Erforderlichkeitsprüfung – bloße Modernisierungs und Effizienzargumente genügen dafür nicht.[14]

FAZIT

Der Entwurf ›delegiert‹ aus unserer Sicht zentrale Schutzwirkungen an generalklauselartige und damit potentiell eingriffsintensive Formeln (»soweit erforderlich«). Die verfassungsrechtliche Rechtsprechung verlangt stattdessen normklare, veröffentlichte Standardisierungen der zulässigen Datenbestände und Methoden sowie ex ante-Kontrollen – nicht erst ex post durch ggfs. lückenhafte Protokollierung. Im Ergebnis droht ein Drift zur projektförmigen Daueranalyse mit faktischer Entgrenzung, vor der auch die Praxis warnt.

Die Schwelle der »bestimmten Tatsachen« für eine schwere Katalogtat ist ein relevantes Verdachtsniveau; angesichts des potenziell sehr hohen Eigengewichts der Plattform fehlt jedoch die gesetzliche Operationalisierung der Verdachtsqualität in Form von konkretisierten, verdichteten Tatsachen und des strikten Anlassbezugs, die das BVerfG bei daten- und methodenoffenen Befugnissen verlangt.

Für wirkliche Transparenz und Waffengleichheit reicht die bloße Protokollierung von SoftwareBezeichnung, Einsatzzeitpunkt und Organisationseinheit nicht aus; erforderlich sind rechtsverbindliche Vorgaben zur Herausgabe von Protokolldaten, Systemdokumentationen, Validierungs- und Fehlerberichten an die Verteidigung, damit gerichtliche Verwertungsprüfungen nicht ins Leere laufen.

Die methodische Einhegung bleibt aus Sicht der Strafverteidigervereinigungen bedenklich unvollständig: Es fehlen der konkrete Ausschluss selbstlernender Systeme, das Verbot maschineller Sachverhaltsbewertungen, eng definierte Ergebnisarten und veröffentlichte Suchmuster-Leitlinien.

Ergänzend zur öffentlichen Debatte bleibt der Hinweis, dass die fehlende explizite Löschpflicht für Referenzdaten sowie der Versuch, das KIVOVerbot über »nonKI«-Scraping zu umgehen, auch hier zentrale Schutzintentionen des EUGesetzgebers konterkarieren; dies sollte der Gesetzgeber klarstellend unterbinden und die unionsrechtlichen Leitplanken vollumfänglich in Tatbestandsmerkmale überführen.

14 Beschl. v. 01.10.2023 - 1 BvR 1160/19 = BVerfGE 169, 332, Rn. 3