DeutscherAnwaltVerein

Stellungnahme

des Deutschen Anwaltvereins vorbereitet durch den Ausschuss Strafrecht und unter Mitwirkung des Ausschusses Recht der Inneren Sicherheit

zum Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz

Entwurf eines Gesetzes zur Änderung der Strafprozessordnung – digitale Ermittlungsmaßnahmen

Stellungnahme Nr.: 26/2026 Berlin, im April 2026

Mitglieder des Ausschusses Strafrecht

- Rechtsanwalt Stefan Conen, Berlin
- Rechtsanwältin Dr. Friederike Goltsche, Münster
- Rechtsanwältin Dr. Gina Greeve, Frankfurt am Main
- Rechtsanwalt Kai Kempgens, Berlin (Berichterstatter)
- Rechtsanwalt Prof. Dr. Stefan Kirsch, Frankfurt am Main
- Rechtsanwältin Dr. Jenny Lederer, Essen
- Rechtsanwalt Prof. Dr. Bernd Müssig, Bonn
- Rechtsanwalt Prof. Dr. Ali B. Norouzi, Berlin (Vorsitzender)
- Rechtsanwältin Dr. Anna Oehmichen, Berlin
- Rechtsanwältin Gül Pinar, Hamburg (stellv. Vorsitzende)
- Rechtsanwalt Prof. Dr. Tilman Reichling, Frankfurt am Main
- Rechtsanwalt Martin Rubbert, Berlin

Zuständig in der DAV-Geschäftsstelle

- Rechtsanwältin Tanja Brexl, Geschäftsführerin, Berlin
- Michael Bimmler, Referent, Berlin

Deutscher Anwaltverein
Littenstraße 11, 10179 Berlin
Tel.: +49 30 726152-0
Fax: +49 30 726152-190
E-Mail: dav@anwaltverein.de

Büro Brüssel
Rue Joseph II 40, Boîte 7B
1000 Brüssel, Belgien
Tel.: +32 2 28028-12
Fax: +32 2 28028-13
E-Mail: bruessel@eu.anwaltverein.de
EU-Transparenz-Registernummer:
87980341522-66

www.anwaltverein.de

Mitglieder des Ausschusses Recht der Inneren Sicherheit

- Rechtsanwältin Lea Voigt, Bremen (Vorsitzende)
- Rechtsanwalt Wilhelm Achelpöhler, Münster
- Rechtsanwalt Dr. David Albrecht, Berlin
- Rechtsanwältin Dr. Lea Babucke, Düsseldorf
- Prof. Dr. Annika Dießner, Berlin (ständiges Gastmitglied im Ausschuss)
- Rechtsanwalt Dr. Nikolas Gazeas, LL.M., Köln
- Rechtsanwalt Dr. Tobias Groscurth, Frankfurt am Main
- Rechtsanwalt Dr. Andreas Grözinger, Köln
- Rechtsanwalt Dr. Mayeul Hiéramente, Hamburg
- Rechtsanwalt Dr. Saleh Ihwas, Frankfurt am Main
- Rechtsanwalt Dr. Arne Klaas, Berlin
- Rechtsanwältin Dr. Regina Michalke, Frankfurt am Main
- Prof. Dr. Mark A. Zöller, München (ständiges Gastmitglied im Ausschuss)

Zuständig in der DAV-Geschäftsstelle

- Rechtsanwalt Max Gröning, Geschäftsführer, Berlin
- Rechtsanwältin Katharina Schmidt-Matthäus, Referentin

Der Deutsche Anwaltverein (DAV) ist der freiwillige Zusammenschluss der deutschen Rechtsanwältinnen und Rechtsanwälte. Der DAV versammelt ca. 60.000 Rechtsanwältinnen und Rechtsanwälte sowie Anwaltsnotarinnen und Anwaltsnotare, die in 253 lokalen Anwaltvereinen im In- und Ausland organisiert sind. Er vertritt die Interessen der deutschen Anwaltschaft auf nationaler, europäischer und internationaler Ebene. Der DAV ist im Lobbyregister für die Interessenvertretung gegenüber dem Deutschen Bundestag und der Bundesregierung zur Registernummer R000952 eingetragen.

A. Einführung

Der vorliegende Gesetzesentwurf ergänzt die Strafprozessordnung um zwei zusätzliche Ermächtigungsnormen, die den Strafverfolgungsbehörden den automatisierten biometrischen Abgleich mit öffentlich zugänglichen Daten aus dem Internet (§98d StPO-E) und die automatisierte verfahrensübergreifende Datenanalyse (§98e StPO-E) ermöglichen sollen.

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

Aus Sicht des Deutschen Anwaltvereins ist der vorgesehene Anwendungsbereich der Ermächtigung zum automatisierten Abgleich biometrischer Daten zu extensiv. Darüber hinaus bedarf es einer Einschränkung des Straftatenkatalogs in Verbindung mit einer Begrenzung auf im Einzelfall schwere Straftaten, der Unterstellung unter einen Richtervorbehalt und einer strengeren Subsidiarität. Zudem sollte die Verwertbarkeit von Erkenntnissen aus automatisierten Abgleichen im Hinblick auf die Intransparenz solcher Anwendungen im Strafprozess ausgeschlossen werden, sodass allenfalls eine Nutzung als Spurenansatz möglich ist. Zuletzt sollten angesichts der Heimlichkeit solche Ermittlungsmaßnahmen diese einer umfassenden Dokumentationspflicht sowie einer turnusmäßigen Evaluierung unterworfen werden. Im Übrigen stellt sich für den Deutschen Anwaltverein die Frage, wie ein automatisierter biometrischer Abgleich mit öffentlich zugänglichen Daten angesichts des europäischen Rechtsrahmens

(Datenschutzgrundverordnung, KI-Verordnung) rechtskonform in der Praxis durchgeführt werden soll.

(Auch) bei der Einführung der automatisierten verfahrensübergreifenden Datenanalyse schießt der Entwurf aus Sicht des Deutschen Anwaltvereins erheblich über das Ziel hinaus. So wären solche Maßnahmen (allenfalls) unter einen Richtvorbehalt und erheblich engere Voraussetzungen zu stellen. Zudem müsste der Einsatz selbstlernender Systeme gesetzlich ausgeschlossen werden. Letztlich darf sich die Legitimation zur übergreifenden Datenanalyse auf keinen Fall – wie es mit dem Entwurf der Fall wäre – auf digitale Beweismittel (TKÜ-Daten, Verkehrsdaten, Mobiltelefondaten, E-Mail-Postfächer) erstrecken. Andernfalls würde die Schaffung eines gigantischen digitalen Beweismittelpools mit zum Teil höchstpersönlichen Daten erlaubt werden, auf den (aus Sicht der Drittbetroffenen) anlasslos und schrankenlos Zugriff genommen werden könnte, obgleich eine solche automatisierte Datenanalyse einen tiefen Eingriff in das Grundrecht auf informationelle Selbstbestimmung darstellt.

Insgesamt ist festzuhalten, dass beide Befugnisnormen legitime Anliegen – nämlich die Personenfahndung anhand von öffentlichen Internetseiten und die Vereinfachung der Abfrage verschiedener bereits vorhandener polizeilicher Auskunftssysteme – zum Anlass nehmen, um völlig uferlose automatisierte Recherchen in teilweise höchstpersönlichen Daten zu legitimieren. So würde die automatisierte Recherche eines tiefgehenden Online-Persönlichkeitsprofils anhand von biometrischen Analysen ebenso ermöglicht, wie die automatisierte Tiefenauswertung jedweder im Besitz der Ermittlungsbehörden befindlichen, anlässlich anderer Strafverfahren, also bei Dritten aufgelaufener Überwachungsdaten und digitaler Beweismittel. Dieser unkontrollierte Zugriff auf solche faktischen Vorratsdaten lässt sich aus Sicht des Deutschen Anwaltvereins angesichts der massiven Tiefe des Grundrechtseingriffs nicht ansatzweise rechtfertigen und würde eine Überwachungsdystopie verwirklichen, die massiv dem Rechtsstaatsprinzip zuwiderläuft.

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

Der automatisierte biometrische Abgleich mit öffentlich zugänglichen Daten aus dem Internet betrifft allen voran den Fall einer automatisierten Gesichtserkennung, da sich vor allem Gesichtsbilder und die zugehörigen personenbezogenen Daten (Name, berufliche Tätigkeit, Wohnort) massenhaft im Internet befinden. Einen solchen Abgleich bieten derzeit nach Kenntnis des Deutschen Anwaltvereins ausschließlich private Unternehmen mit Sitz außerhalb der Europäischen Union an, so die Unternehmen PimEyes und Clearview. Im Inland ist bislang lediglich ein automatisierter Abgleich mit polizeilichen Datenbanken, etwa mit der Datenbank INPOL, möglich, der in der Praxis bislang ebenfalls ohne explizite Rechtsgrundlage erfolgt und insofern auch dringend einer Regelung zugeführt werden sollte.

Die Debatte um die Nutzung entsprechender automatisierter Tools wurde im Rahmen der Festnahme der langjährig als mutmaßliches Ex-RAF-Mitglied gesuchten Daniela Klette intensiviert. Zuvor hatte ein Investigativjournalist die Beschuldigte anhand von Fahndungsfotos über die von einem Privatkonzern betriebene Gesichtsdatenbank PimEyes ausfindig gemacht. Seitdem mehren sich die Stimmen, auch Ermittlungsbehörden die Nutzung von KI-gestützten Gesichtsdatenbanken ähnlich PimEyes oder Clearview AI zu ermöglichen.

Bislang gestatten die strafprozessualen Regelungen allenfalls einen manuellen Abgleich biometrischer Daten mit öffentlich zugänglichen Daten aus dem Internet als weniger gravierenden Eingriff in Grundrechte. Der vorliegende Entwurf sieht nun eine umfassende Ermächtigung des automatisierten biometrischen Abgleichs mit Internetdaten vor.

Ein früherer Entwurf aus dem Jahre 2024[1] unterwarf entsprechende Maßnahmen damals noch engeren Grenzen. So waren solche Maßnahmen nur zur

[1] https://dserver.bundestag.de/btd/20/128/2012806.pdf

Identitätsfeststellung und Ermittlung des Aufenthaltsorts bei Katalogtaten des § 100a Abs. 2 StPO, die im Einzelfall schwer wogen, unter Richtervorbehalt vorgesehen. Der vorliegende Entwurf geht weit darüber hinaus.

Der automatisierte biometrische Abgleich, insbesondere der Einsatz von Gesichtserkennung zur Strafverfolgung greift stets in das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) ein – auch bei Personen, bei denen kein Treffer erzielt wird, sondern die sich in einer Abgleichdatenbank befinden. Zwar wird die Intensität dadurch abgemildert, dass die Daten aus öffentlich zugänglichen Quellen stammen, die Rechtsprechung des Bundesverfassungsgerichts sieht jedoch dennoch einen Schutz dieser personenbezogenen Daten vor. Die Eingriffsintensität ist als hoch einzustufen, da die Maßnahmen eine große Streubreite aufweisen, regelmäßig verdeckt durchgeführt werden und anlasslos in biometrische Daten mit starkem Personenbezug eingreifen. Der Einsatz von KI, wie es bei allen Anwendungen zur automatisierten Bilderkennung der Fall ist, verstärkt die Eingriffsintensität erheblich, da er den Abgleich mit Milliarden von Bildern erst ermöglicht und damit Streubreite sowie Personenbezug potenziert. Insbesondere ist hervorzuheben, dass der automatische biometrische Abgleich mit im Internet verfügbaren Bildern eine weit höhere Streubreite und Eingriffsintensität bedeutet als ein solcher Abgleich mit polizeilichen Datenbanken. Denn in den Abgleichdatenbanken, die private Unternehmen mit im Internet verfügbaren Gesichtsbildern geschaffen haben, befinden sich weit mehr Gesichtsbilder als in staatlichen Datenbanken. Während das BKA im Jahr 2023 von ca. 6 Millionen Gesichtsbildern in der Datenbank sprach, verfügt etwa das Unternehmen Clearview Stand jetzt 2025 über einen Datenbestand von ca. 60 Milliarden Gesichtsbildern weltweit. Dies bezieht nicht nur mehr Personen in eine Suchanfrage ein, sondern ermöglicht auch eine viel höhere Informationsdichte durch die Einbeziehung von Informationen aus sozialen Medien.
Der deutsche Anwaltverein geht daher unter Berücksichtigung der Rechtsprechung des Bundesverfassungsgerichts zum Grundrecht auf informationelle Selbstbestimmung und unter Berücksichtigung insbesondere des Urteils des Bundesverfassungsgerichts in der Sache Hessen-Data[2] von einem erheblichen Grundrechtseingriff durch die vorgesehene

[2] 1 BvL 3/22

Ermächtigungsnorm aus. Entsprechend sind solche Maßnahmen nur unter Einhaltung strenger materieller wie formeller Voraussetzungen möglich.

I. Zu § 98d Abs. 1 StPO-E

Der Deutsche Anwaltverein versteht die Begrenzung auf den Recherchekreis auf „*öffentliche zugängliche biometrische Daten*“ dahingehend, dass jedenfalls keine Social-Media-Daten nutzbar gemacht werden sollen, die einem beschränkten Nutzerkreis zugänglich gemacht werden sollten[3], was zu begrüßen ist.

Die Erweiterung des Einsatzzwecks eines automatisierten biometrischen Abgleichs neben der Identitätsfeststellung und zur Ermittlung des Aufenthaltsorts des Beschuldigten oder eines Zeugen auf die „Erforschung des Sachverhalts“ (im Vergleich zum Gesetzesentwurf 2024) stellt die Maßnahme unter eine Generalklausel. Dies gestattet letztlich den Einsatz automatisierter biometrischer Abgleiche zu jedwedem Ermittlungszweck und nicht nur zur Identifizierung oder Lokalisierung von Personen. Legitimiert wären sämtliche Recherchemaßnahmen, die in ihrer Gesamtheit die Erstellung eines umfassenden Bewegungs- und Persönlichkeitsprofils des Beschuldigten bis hin in seine höchstpersönlichen Beziehungen und Lebensbereichen zulassen. Gerade dann, wenn eine Rechtsgrundlage so konzipiert ist, dass sie die Erstellung umfassender Bewegungs- und Persönlichkeitsprofile ermöglicht, markiert dies nach der Rechtsprechung des Bundesverfassungsgerichts die absolute Grenze zulässiger und rechtfertigungsfähiger digitaler Ermittlungsmaßnahmen. Die Streubreite ist extrem. Der Aspekt, dass Betroffene in vielen Fällen gar keinen Einfluss auf die Fertigung und Veröffentlichung von Bilddarstellungen haben, verdeutlich die Tiefe des damit verbundenen Grundrechtseingriffs. Aus Sicht des Deutschen Anwaltvereins lässt sich ein solcher Eingriff nicht mit der geltenden Verfassungsgerichtsrechtsprechung vereinbaren. Die vorgesehene Anwendung automatisierter biometrischer Abgleiche auch zur Erforschung des Sachverhaltes sollte daher gestrichen werden.

[3] so auch die Entwurfsbegründung, S. 12

(Auch) der gewählte Eingriffsvorbehalt lässt sich aus Sicht des Deutschen Anwaltvereins selbst bei bloßen Maßnahmen der Fahndung und Identitätsfeststellung nicht mit verfassungsrechtlichen Vorgaben[4] vereinbaren. Der Katalog des § 100a Abs. 2 StPO zieht den Kreis der Anlassdelikte erheblich zu weit, da es sich teilweise nicht um den Schutz herausragender Schutzgüter handelt. Darunter fallen auch bestimmte Verstöße gegen das Konsumcannabisgesetz (Nr. 7a), Formen der Veruntreuung von Arbeitsentgelten (Nr. 1 lit. q) oder Sozialhilfebetrug (Nr. 1 lit. n) und bestimmte Vorfeldstraftaten. Darüber hinaus öffnet der Entwurf durch den Gebrauch der Formulierung „*insbesondere*“ für weitere Straftaten erheblicher Bedeutung. Das BVerfG betont, dass bei tief in die Privatsphäre eingreifenden Überwachungsmaßnahmen eine besonders strenge Eingriffsschwelle und der Schutz überragend wichtiger Rechtsgüter unumgänglich sind[5]. Aus Sicht des Deutschen Anwaltvereins müsste der Anwendungsbereich zumindest auf den Katalog des § 100b Abs. 2 StPO eingeschränkt werden[6]. Darüber hinaus bedürfte es einer zusätzlichen Beschränkung auf Taten, die im Einzelfall schwer wiegen.

§ 98d Abs. 1 Nr. 2 StPO-E sieht vor, dass die Maßnahme nur zulässig ist, wenn die Sachverhaltsaufklärung „*auf andere Weise wesentlich erschwert oder aussichtslos wäre*". Dies wird der unionsrechtlichen Anforderung der „*unbedingten*" Erforderlichkeit im Sinne einer verschärften conditio-sine-qua-non aus Art. 10 der Richtlinie 2016/680/EU und § 48 Abs. 1 BDSG nicht gerecht[7]. Dort ist verlangt, dass der Erkenntnisgewinn sicher ausgeschlossen sein muss auf andere Weise erlangt werden zu können. Zur Gewährleistung dieser unionsrechtlichen Anforderung ist die Maßnahme daher unter die Subsidiarität der unbedingten Erforderlichkeit zu stellen.

II. Zu § 98d Abs. 2 StPO-E

Aus Sicht des Deutschen Anwaltvereins ist das Bemühen zu begrüßen, durch die in § 98d Abs. 2 StPO-E normierte Dokumentationspflicht eine ansatzweise Transparenz der Nutzung zu schaffen. Dies greift aber bei Weitem zu kurz.

---

4 vgl. BVerfG, Beschluss des Ersten Senats vom 18. Dezember 2018, 1 BvR 142/15, Rn. 51)
5 1 BvL 3/22, Rz. 96
6 so auch Rückert, StV 2025, 350 - 356
7 vgl. Rückert, StV 2025, 350 - 356

Angesichts der gerade bei Gesichtsidentifikationen zu erwartenden Priming-Effekte bei der nachfolgenden menschlichen Bewertung – beispielsweise in der Hauptverhandlung – ist eine präzise Dokumentation der konkreten Suchanfragen einschließlich des verwendeten Referenzmaterials und der jeweiligen Suchergebnisse (einschließlich Negativergebnisse) für die Bewertung des Beweiswertes unabdingbar. Obgleich § 168b Abs. 1 StPO die Ermittlungsbehörden ohnehin zur Protokollierung ihrer Ermittlungsschritte verpflichtet, erscheint in Fällen des automatisierten biometrischen Abgleichs die spezialgesetzliche bloße Verpflichtung zur Angabe der „Formalien“ nicht ansatzweise ausreichend. Aus den oben dargestellten Gründen sind die Ermittlungsbehörden vielmehr zur Schaffung einer Datenlage zu verpflichten, die eine vollständige Reproduktion des gesamten Suchvorgangs (einschließlich unergiebiger Anfragen) ermöglicht. Darüber hinaus sollte klargestellt werden, dass die Dokumentation auch in der Ermittlungsakte festgehalten werden muss.

Angesichts der Heimlichkeit und Intransparenz des automatisierten biometrischen Abgleichs erscheint aber eine bloße Dokumentation im Einzelfall noch nicht ausreichend. Vielmehr sollte vorgesehen werden, dass turnusmäßig (etwa alle drei Jahre) die im Einsatz befindlichen Abgleichsysteme evaluiert werden. U. a. sollte evaluiert werden, welche Systeme welchen Anbieters, wie oft, mit welchem Zweck und mit welchem Erfolg eingesetzt wurden.

III. Zu § 98d Abs. 4 StPO-E

Nicht ausreichend ist eine Beschränkung der Anordnungskompetenz in Regelfällen auf die Staatsanwaltschaft. Erforderlich erscheint angesichts der erheblichen Eingriffstiefe eine Anordnung durch den Ermittlungsrichter, wie sie auch hinsichtlich anderer, ähnlich eingriffsintensiver Maßnahmen strafprozessual installiert ist. Eine solche verfahrensrechtliche Absicherung erscheint nicht nur vor dem Hintergrund der erheblichen Eingriffsintensität der vorgesehene Ermittlungsmaßnahme erforderlich. Sie erscheint insbesondere angesichts der Intransparenz und Heimlichkeit solcher Ermittlungsmaßnahmen dringend notwendig. Eine Zuweisung der Anordnungskompetenz zum Ermittlungsrichter würde sicherstellen, dass solche Ermittlungsmaßnahmen zwingend in der Ermittlungsakte erfasst und ihre aus der

Sicht der Ermittlungsbehörden gegebene Erforderlichkeit dokumentiert würde. Dies würde die Transparenz und damit verbunden die Nachprüfbarkeit solcher Maßnahmen erheblich erhöhen und damit den Grundrechtseingriff mindern. Erforderlich wären zudem formelle Anforderungen an die Begründung.

IV. Weitere erforderliche Einschränkungen und Klarstellungen

Wünschenswert wäre zudem, wenn in der Ermächtigungsnorm klarstellend aufgenommen würde, dass nur solche Systeme zum automatisierten biometrischen Abgleich eingesetzt werden dürfen, die den Anforderungen der KI-Verordnung entsprechen: Die retrograde KI-Gesichtserkennung ist nach Art. 6 Abs. 2 KI-VO i.V.m. Anhang III Nr. 1 a) ein sog. Hochrisiko-KI-System und damit den dafür geltenden Restriktionen der KI-VO unterworfen. Die dortigen Vorgaben der Art. 8 bis 15 KI-VO adressieren die spezifischen Risiken von KI-Systemen. Sie verpflichten Anbieter und Betreiber im Wesentlichen zur Einführung von Risikomanagementsystemen, zur sorgfältigen Auswahl von Trainingsdaten sowie zur Einhaltung von Dokumentations- und Protokollierungspflichten. Ergänzend werden ein Mindestmaß an inhaltlicher Korrektheit und Nachvollziehbarkeit der KI-Ausgaben verlangt sowie eine wirksame menschliche Aufsicht einschließlich der Plausibilitätskontrolle der erzielten Ergebnisse vorgeschrieben.

Zudem sollte die Verwertbarkeit von Erkenntnissen aus automatisierten Abgleichen im Hinblick auf die Intransparenz solcher Anwendungen im Strafprozess ausgeschlossen werden, sodass allenfalls eine Nutzung als Spurenansatz möglich ist. Die derzeitigen Systeme zum automatisierten biometrischen Abgleich beruhen alle auf Techniken der künstlichen Intelligenz. Diesen Systemen ist eine Intransparenz inhärent (sogenannter Blackbox Effekt), d. h. es ist nicht nachvollziehbar, weshalb das System einen bestimmten Treffer erzielt hat, zum Beispiel weshalb eine bestimmte Person als verdächtige Person identifiziert wird. Solche Treffer könnten daher nicht begründbar als Beweismittel eingeführt werden. Insofern sollte explizit ausgeschlossen werden, dass die von biometrischen Abgleichsystemen erzielten Treffer zur Beweisverwertung herangezogen werden dürfen.

Zuletzt stellt sich für den Deutschen Anwaltverein die Frage, wie ein automatisierter biometrische Abgleich mit öffentlich zugänglichen Daten angesichts des europäischen Rechtsrahmens insbesondere auf der Grundlage der unmittelbar geltenden Datenschutzgrundverordnung sowie der KI-Verordnung rechtskonform in der Praxis durchgeführt werden soll.

Nach Verständnis des Deutschen Anwaltvereins sieht der Entwurf keine Ermächtigung zum Aufbau einer biometrischen Referenzdatenbank auf Vorrat vor. Der eigene Aufbau einer solchen biometrischen „Bürgerdatenbank“ wäre wohl kaum mit deutschem Verfassungsrecht vereinbar. Denn durch den Aufbau einer Biometrik-Datenbank wären überwiegend Grundrechte von Millionen unbeteiligten Personen betroffen, die keinen Anlass für polizeiliche Überwachung gegeben haben. Zudem untersagt Art. 5 Abs. 1 e KI-VO als verbotene Praktik:

> *„das Inverkehrbringen, die Inbetriebnahme für diesen spezifischen Zweck oder die Verwendung von KI-Systemen, die Datenbanken zur Gesichtserkennung durch das ungezielte Auslesen von Gesichtsbildern aus dem Internet oder von Überwachungsaufnahmen erstellen oder erweitern“.*

Damit ist nach Ansicht des Deutschen Anwaltvereins explizit klargestellt, dass der Aufbau einer biometrischen Referenzdatenbank staatlicherseits unionsrechtswidrig ist.

Daneben wäre nach Ansicht des Deutschen Anwaltvereins auch ein Zugriff auf Angebote privater Unternehmen wie PimEyes oder Clearview AI unionsrechtswidrig. Die Praktiken insbesondere von Clearview wurden bereits von mehreren Datenschutzbehörden innerhalb der Europäischen Union mit Bußgeldern belegt. Das Unternehmen PimEyes hat seinen Unternehmenssitz vor Jahren aus der Europäischen Union heraus nach wohl derzeit Dubai verlegt. Ein Rückgriff auf private Unternehmen und deren Geschäftspraktiken, erscheint aus Sicht der Deutschen Anwaltsvereins ausgeschlossen. Zudem erscheint es nicht vorstellbar, dass in Zeiten eines Strebens nach mehr digitaler Souveränität innerhalb der Europäischen Union eine solche Abhängigkeit bei Ermittlungsmaßnahmen gewünscht ist.

Auch zur grundsätzlichen Sicherstellung der Anwendbarkeit des EU-Datenschutzregimes bedarf es zudem der Vorgabe der Auftragsdatenverarbeitung in der EU bzw. im Schengen Raum.

C. § 98e StPO-E: Automatisierte verfahrensübergreifende Datenanalyse

Das Anliegen des Gesetzentwurfs, ein derzeit teilweise noch „*unverbundenes Nebeneinander zahlreicher automatisierter Dateien und Datenquellen*“[8] leichter durchsuchbar zu gestalten, erscheint auf den ersten Blick nachvollziehbar. Die mit dem Entwurf des §98e StPO-E eingeräumten Ermächtigungsgrundlagen gehen aber sehr weit über dieses Anliegen hinaus.

I. Reichweite der Entscheidung des BVerfG 1 BvR 1547/19

Kaum denkbar erscheint, dass sich die in der Grundsatzentscheidung 1 BvR 1547/19 vom Bundesverfassungsgericht aufgestellten Bedingungen, unter denen die Verfassungsmäßigkeit von automatisierten Analyseplattformen überhaupt möglich erscheint, ohne weiteres auf den repressiven Bereich der Strafprozessordnung übertragen lassen. Die Entscheidung selbst lässt diesen Anknüpfungspunkt gänzlich außer Acht. Soweit der Gesetzesentwurf nicht nur eine Vernetzung bereits vorhandener polizeilicher Vorgangsdaten und Falldaten ermöglichen soll, sondern einen Zugriff auf in anderen Strafverfahren gewonnenen Beweisdaten legitimieren soll, geht die Eingriffstiefe deutlich über die in der Grundsatzentscheidung diskutierte Eingriffskonstellation hinaus.

II. Einsatz zur zentralen Auswertung von Vorgangs- und Falldaten

Soweit es um die Möglichkeit der übergreifenden maschinellen Suche in polizeilichen Informationssystemen geht, besteht bereits de lege lata eine Ermächtigung aus § 98c StPO. Die Nutzung einer automatisierten

[8] vgl. S. 6 der Entwurfsbegründung

Analyseanwendung stellt nach der Grundsatzentscheidung einen schwerwiegenden Eingriff in die informationelle Selbstbestimmung der Betroffenen dar und ist nur unter engen Voraussetzungen gerechtfertigt[9]. Dies führt nach den dortigen Ausführungen zum Erfordernis einer strengen Begrenzung des Eingriffsanlasses[10].

Obgleich der Entwurf den Einsatzbereich auf „*im Einzelfall schwerwiegende Straftaten*“ begrenzt, wird die Implementierung des Kataloges des § 100a Abs. 2 StPO diesen Vorgaben aus Sicht des Deutschen Anwaltvereins nicht gerecht. Unter den Katalog fallen auch bestimmte Verstöße gegen das Konsumcannabisgesetz (Nr. 7a), Formen der Veruntreuung von Arbeitsentgelten (Nr. 1 lit. q) oder Sozialhilfebetrug (Nr. 1 lit. n) und bestimmte Vorfeldstraftaten, die das Kriterium des Schutzes besonders gewichtiger Rechtsgüter nicht erfüllen. Zudem erscheint das Eingrenzungskriterium „*im Einzelfall schwerwiegende Straftaten*“ vor diesem Hintergrund zu unbestimmt.

Zudem bedürfte es eines Richtervorbehalts, um die effektive Kontrolle und die Sicherstellung des Verhältnismäßigkeitsprinzips zu gewährleisten.

Außerdem sollte die Verwertbarkeit von Analyseerkenntnissen aus automatisierten Abgleichen im Strafprozess ausgeschlossen werden, sodass allenfalls eine Nutzung als Spurenansatz möglich ist. Die verwendeten automatisierten KI-Systeme sind grundsätzlich als intransparent zu qualifizieren. Treffer könnten daher nicht begründbar als Beweismittel eingeführt werden.

Grundsätzlich zu begrüßen ist die Normierung einer Protokollierungspflicht in Absatz 5 von § 98e StPO-E. Diese greift aus Sicht des Deutschen Anwaltvereins aber zu kurz. Obgleich § 168b Abs. 1 StPO die Ermittlungsbehörden ohnehin zur Protokollierung ihrer Ermittlungsschritte verpflichtet, erscheint auch hier die Verpflichtung zur Dokumentation der „Formalien“ nicht ansatzweise ausreichend. Die Ermittlungsbehörden sind vielmehr dazu zu verpflichten, die genaue Suchanfrage einschließlich aller durchsuchten Datenquellen im Einzelnen und aller

[9] 1 BvR 1547/19 Rz. 104
[10] 1 BvR 1547/19 Rz. 106

Ergebnisse aktenkundig zu machen, um den Suchvorgang im weiteren Verlauf des Verfahrens nachvollziehbar zu machen.

III. Einsatz von KI

Der etwaige Einsatz von selbstlernenden Systemen würde die Eingriffsintensität in einer Weise erhöhen, dass sich solche Maßnahmen als ungerechtfertigt erweisen. Der Gesetzgeber muss daher einschränkende Vorgaben zur Methode der automatisierten Datenanalyse oder -auswertung im Gesetz selbst regeln[11]. Der Einsatz selbstlernender Systeme muss dafür im Gesetz ausdrücklich ausgeschlossen sein[12]. Zudem muss eine Begrenzung der Abgleichmöglichkeit auf Analysetools, die einen einfachen Datenabgleich in automatisierter Form vorsehen, ausdrücklich gesetzlich normiert werden[13].

Zur Sicherstellung der Anwendbarkeit des EU-Datenschutzregimes bedarf es zudem der Vorgabe der Auftragsdatenverarbeitung in der EU bzw. im Schengen Raum.

IV. Einsatz zur automatisierten Auswertung von Beweisdaten (u.a. TKÜ, Asservate etc.)

Soweit im Rahmen der automatisierten Auswertung auch auf Beweisdaten zugegriffen werden soll, widerspricht dies der Grundkonstruktion der Strafprozessordnung und verfassungsrechtlichen Grundsätzen.

So soll nach dem vorliegenden Gesetzentwurf eine automatisierte Analyse auch die aufgrund von Maßnahmen nach den §§ 100a, 100f, 100g, 100k Abs. 1 und 2, 100i StPO in anderen Strafverfahren gewonnenen und aus Asservaten stammenden personenbezogenen Daten ergänzend einbezogen werden, soweit dies erforderlich ist.

---

[11] vgl. 1 BvR 1547/19, Rz. 120
[12] vgl. 1 BvR 1547/19, Rz 121
[13] vgl. 1 BvR 1547/19, Rz 121

Dies bedeutet faktisch die Legitimation einer automatisierten Durchsicht und Analyse fast sämtlicher in Drittverfahren gewonnenen und vorhandenen digitalen Beweisdaten. Ermittlungsbehörden könnten daher umfangreiche automatisierte Tiefenrecherchen im tatsächlich vorhandenen Vorrat aller aus Verfahren gegen Dritte vorliegenden digitalen Überwachungs- und Beweisdaten anstellen.

Die Beweisdaten der Drittverfahren wurden indes gar nicht aus Anlass des Abfrageverfahrens und erst nach einer hierauf bezogenen Anlass- und Verhältnismäßigkeitsprüfung gewonnen. Umgekehrt betrifft die Analyse Persönlichkeitsrechte Dritter, die im Anlassverfahren meist keinen Anlass für eine Auswertung ihrer – im Drittverfahren gewonnenen – Daten gegeben haben.

Das Bundesverfassungsgericht hat in der Grundsatzentscheidung BVerfG 2 BvR 1027/02[14] 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 auch, dass vor Beginn einer Durchsicht überhaupt ein Auffindeverdacht in der Form feststehen muss, in den konkret sichergestellten Daten seien überhaupt verfahrensrelevante Informationen vorhanden.[15] Auch in der Entscheidung BVerfG 2 BvR 497/03 wurde noch einmal ausdrücklich betont, auch bereits bei der Durchsicht sei zu berücksichtigen, die Gewinnung überschießender und vertraulicher, für das Verfahren aber bedeutungsloser Informationen im Rahmen des Vertretbaren zu vermeiden. Eine Durchsicht elektronischer Beweismittel ohne jeden Auffindeverdacht verbietet sich nach diesen Grundsätzen von vornherein.

Dieser Rechtsgedanke ergibt sich auch aus den strafprozessualen Vorgaben hinsichtlich einer Umwidmung von Beweismitteln. § 479 StPO stellt eine Verwertung in anderen Strafverfahren unter den Vorbehalt der hypothetischen Eingriffslegitimation. Dies bedeutet selbstverständlich auch, dass nur grundsätzlich verwendbare Daten überhaupt einer Analyse unterzogen werden dürfen.

---

[14] BVerfG 2 BvR 1027/02 (= NJW 2005, 1917)
[15] vgl. BVerfG 2 BvR 1027/02 (= NJW 2005, 1917); Szesny, WiJ 2012, 228 ff.

Eine die automatisierte verfahrensübergreifende Analyse von digitalen Beweisdaten erlaubende Ermächtigung müsste (wenn überhaupt) daher sicherstellen, dass für jede Datenquelle bereits vor dem Analysevorgang geprüft und festgehalten wird, wieso hinsichtlich des konkret durchsuchten Beweismittels ein Auffindeverdacht bestehen soll und wieso eine Verwertung überhaupt in Betracht kommt. Die Datenquellen sind in dieser Form gesetzlich zu begrenzen. Eine Begründungspflicht ist ausdrücklich zu normieren.

Dies gilt insbesondere auch deshalb, weil durch eine Analysemaßnahme tief in Rechte unbeteiligter Dritter[16] eingegriffen wird. Völlig offen bleibt zudem, wie betroffene Dritte im gebotenen Umfang an der Maßnahme beteiligt werden sollen[17], insbesondere wie eine Benachrichtigung von einem Datenzugriff erfolgen soll.

Zudem würden Schutzrechte von Berufsgeheimnisträgern ebenso wenig gewährleistet wie der verfassungsrechtlich gebotene Kernbereichsschutz.

(Jedenfalls) soweit der vorliegende Entwurf eine Analyse der Inhalte von Asservaten und Erkenntnissen aus Überwachungsmaßnahmen (§§ 100a, 100f, 100g, 100k Absatz 1 und 2, § 100i StPO) ermöglicht und die Kontrolle (offenbar) allein der späteren Ex-Post-Bewertung überlassen möchte, dürfte aus diesen Gründen nicht ansatzweise eine verfassungsrechtliche Vereinbarkeit gegeben sein.

[16] nämlich beispielsweise die Beschuldigten der Drittverfahren, gegen die im Anlassverfahren gar kein Tatverdacht besteht

[17] vgl. BVerfG 2 BvR 902/06

Verteiler

- Bundesministerium der Justiz und für Verbraucherschutz
- Bundesministerium des Innern
- Ausschuss für Recht und Verbraucherschutz des Deutschen Bundestages
- Finanzausschuss und Ausschuss für Digitales und Staatsmodernisierung des Deutschen Bundestages
- Innenausschuss des Deutschen Bundestages
- Arbeitsgruppen Recht der im Deutschen Bundestag vertretenen Parteien
- Arbeitsgruppen Inneres der im Deutschen Bundestag vertretenen Parteien
- Fraktionen des Deutschen Bundestages
- Justizministerien der Länder
- Innenministerien der Länder
- Rechts- und Innenausschüsse der Landtage

- Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
- Landesdatenschutzbeauftragte
- Bundesgerichtshof
- Der Generalbundesanwalt beim Bundesgerichtshof
- Europäische Kommission, Vertretung in Deutschland
- Rechtsausschuss des Bundesrates

- Bundesrechtsanwaltskammer
- Bundesverband der Freien Berufe
- Deutsches Institut für Menschenrechte
- Gesellschaft für Freiheitsrechte
- Deutscher Richterbund
- Gewerkschaft der Polizei
- Deutsche Polizeigewerkschaft
- Bund Deutscher Kriminalbeamter
- Deutscher Juristentag
- Republikanischer Anwältinnen- und Anwälteverein e. V.
- Deutscher Juristentag
- Gesellschaft für Freiheitsrechte (GFF)
- Innocence Project Deutschland – Fehlurteil und Wiederaufnahme e.V.
- Kriminalpolitischer Kreis
- Arbeitskreis Alternativ-Entwurf
- ver.di, Bereich Recht und Rechtspolitik
- Deutsche Vereinigung für Jugendgerichte und Jugendgerichtshilfen
- Strafverteidiger-Forum (StraFo)
- Neue Zeitschrift für Strafrecht (NStZ)
- Strafverteidiger (StV)
- Neue Richter*innenvereinigung e.V.
- Bundesverband Ehrenamtlicher Richterinnen und Richter e.V.
  = Deutsche Vereinigung der Schöffinnen und Schöffen =
- Deutscher Strafverteidiger e.V.
- Regionale Strafverteidigervereinigungen
- Organisationsbüro der Strafverteidigervereinigungen und -initiativen
- Deutscher Juristinnenbund e.V. (djb)
- Wirtschaftsstrafrechtliche Vereinigung e.V. (WisteV)

- Arbeitskreise Recht der im Bundestag vertretenen Parteien
- Vors. des Strafrechtsausschusses des KAV und des BAV
- Strafrechtsausschuss des Deutschen Anwaltvereins
- Geschäftsführender Ausschuss der Arbeitsgemeinschaft Strafrecht des Deutschen Anwaltvereins
- Strafrechtsausschuss und Strafprozessrechtsausschuss der Bundesrechtsanwaltskammer

- Mitglieder des Vorstandes des Deutschen Anwaltvereins
- Vorsitzenden der Landesverbände des Deutschen Anwaltvereins
- Vorsitzenden der Gesetzgebungsausschüsse des Deutschen Anwaltvereins
- Mitglieder des Ausschusses Recht der Inneren Sicherheit des Deutschen Anwaltvereins
- Vors. des FORUM Junge Anwaltschaft des DAV

<u>Presse</u>

- KriPoZ Kriminalpolitische Zeitschrift
- NJW
- Frankfurter Allgemeine Zeitung
- Süddeutsche Zeitung
- Berliner Verlag GmbH
- Hamburger Abendblatt
- Der Tagesspiegel
- Der Spiegel
- Juris Newsletter
- JurPC
- Netzpolitik.org
- Heise
- LTO
- Neue Zürcher Zeitung
- Frankfurter Rundschau
- Zeit
- beck-online
- Neue Zeitschrift für Verwaltungsrecht
- Die Öffentliche Verwaltung
- Deubner Verlag, LexisNexis, Verlag Dr. Otto Schmidt, Wolters-Kluwe Online, ZAP Verlag
- Zeitschrift für Rechtspolitik (ZRP)
- Kriminalpolitische Zeitschrift (KriPoZ)
- HRR-Strafrecht
- Zeitschrift für Internationale Strafrechtswissenschaft (ZfIStw)
- Neue Kriminalpolitik (NK)
- Zeitschrift für Wirtschafts- und Steuerstrafrecht (wistra)
- Neue Zeitschrift für Wirtschafts-, Steuer- und Unternehmensstrafrecht (NZWiSt)
- Strafverteidiger-Forum (StraFo)
- Neue Zeitschrift für Strafrecht (NStZ)
- Strafverteidiger (StV)