BUNDESRECHTSANWALTSKAMMER

Stellungnahme Nr. 21
April 2026

Entwurf eines Gesetzes zur Änderung der Strafprozessordnung – digitale Ermittlungsmaßnahmen

Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit

Entwurf eines Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse zur Abwehr von Gefahren des internationalen Terrorismus

Mitglieder des Ausschusses Strafrecht (Strauda):

Rechtsanwältin Dr. Carolin Arnemann
Rechtsanwalt Prof. Dr. Jan Bockemühl
Rechtsanwalt Prof. Dr. Alfred Dierlamm
Rechtsanwalt Prof. Dr. Björn Gercke
Rechtsanwalt Dr. Mayeul Hiéramente (Berichterstatter)
Rechtsanwalt Thomas C. Knierim (Berichterstatter)
Rechtsanwalt Dr. Daniel M. Krause
Rechtsanwältin Theres Kraußlach
Rechtsanwalt Prof. Dr. Holger Matt (Vorsitzender)
Rechtsanwalt Prof. Dr. Ralf Neuhaus
Rechtsanwalt Prof. Dr. Tido Park
Rechtsanwältin Dr. Hellen Schilling
Rechtsanwalt Dr. Jens Schmidt
Rechtsanwältin Dr. Annette von Stetten

Rechtsanwältin Leonora Holling, Schatzmeisterin Bundesrechtsanwaltskammer

Mitglieder des Ausschusses Strafprozessrecht:

Rechtsanwalt Dr. Matthias Dann
Rechtsanwalt Prof. Dr. Michael Gubitz
Rechtsanwältin Dr. Vera Hofmann
Rechtsanwalt Prof. Dr. Christoph Knauer (Vorsitzender und Berichterstatter)
Rechtsanwalt Dr. jur. Andreas Minkoff

Rechtsanwalt Maximilian Müller, LL.M.
Rechtsanwalt Jürgen Pauly
Rechtsanwältin Anette Scharfenberg
Rechtsanwältin Dr. Alexandra Schmitz
Rechtsanwältin Stefanie Schott
Rechtsanwalt Prof. Dr. Gerson Trüg

Rechtsanwältin Leonora Holling, Schatzmeisterin Bundesrechtsanwaltskammer
Rechtsanwältin Eva Melina Buchmann, Bundesrechtsanwaltskammer

Mitglieder des Ausschusses Datenschutzrecht:

Rechtsanwalt Klaus Brisch, LL.M., Köln
Rechtsanwalt Malte Dedden, Kehl
Rechtsanwalt Michael Dreßler, Erlangen
Rechtsanwalt Peter Hense, Leipzig
Rechtsanwalt Prof. Dr. jur. Armin Herb, Stuttgart (Vorsitzender)
Rechtsanwältin Heike Kraus, MLE, LL.M., Rauenberg
Rechtsanwalt Jörg Martin Mathis, Koblenz
Rechtsanwältin Simone Rosenthal, Berlin
Rechtsanwalt Dr. Hendrik Schöttle, München
Rechtsanwalt Sebastian Schulz, Berlin
Rechtsanwalt Dr. Volker Schumacher, Düsseldorf

Rechtsanwalt André Haug, Vizepräsident Bundesrechtsanwaltskammer
Rechtsanwalt Sebastian Aurich

Mitglieder des Ausschusses Menschenrechte:

Rechtsanwalt Dr. Sebastian Cording, Hamburg (Berichterstatter)
Rechtsanwalt Detlev Heyder, Freiburg
Rechtsanwältin Ingrid Hönlinger, Ludwigsburg
Rechtsanwalt Dr. Lucas Jürss, Düsseldorf
Rechtsanwalt Prof. Dr. Remo Klinger, Berlin
Rechtsanwältin Dr. Regina Michalke, Frankfurt/Main
Rechtsanwältin Dr. Margarete Mühl-Jäckel, LL.M. (Harvard), Potsdam (Vorsitzende)
Rechtsanwältin Stephanie Schlund, Forchheim

Rechtsanwalt und Notar Dr. Thomas Remmers, Vizepräsident Bundesrechtsanwaltskammer
Rechtsanwalt Sven Krautschneider, Bundesrechtsanwaltskammer

Verteiler: Bundesministerium der Justiz
Bundesministeriums des Innern, für Bau und Heimat
Beauftragte der Bundesregierung für Migration, Flüchtlinge und Integration
Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
Landesdatenschutzbeauftragte der Länder
Ausschuss für Recht- und Verbraucherschutz des Deutschen Bundestages
Ausschuss für Inneres und Heimat des Deutschen Bundestag
Fraktionsvorsitzende der CDU/CSU, SPD, BÜNDNIS 90/DIE GRÜNEN, DIE LINKE
Rechtspolitischen Sprecher der Fraktionen CDU/CSU, SPD, BÜNDNIS 90/DIE GRÜNEN, DIE LINKE
Arbeitskreise Recht der Bundestagsfraktionen
Arbeitsgruppen Menschenrechte und humanitäre Hilfe der im Deutschen Bundestag vertretenen Parteien
Landesjustizminister/Justizsenatoren der Länder
Innenministerien und Senatsverwaltungen für Inneres der Länder
Bundesgerichtshof
Rechtsanwaltskammern
Bundesverband der Freien Berufe
Bundesnotarkammer
Bundessteuerberaterkammer
Patentanwaltskammer
Deutscher Anwaltverein
Deutscher Juristinnenbund
Deutscher Notarverein
Deutscher Richterbund
Neue Richtervereinigung e.V.
Deutscher Steuerberaterverband e. V.
Wirtschaftsprüferkammer
Institut der Wirtschaftsprüfer in Deutschland e.V.
Bund Deutscher Kriminalbeamter
Verbraucherzentrale Bundesverband e.V.
Deutscher Juristentag e.V.
Gesellschaft für Datenschutz und Datensicherheit e.V.
Berufsverband der Datenschutzbeauftragten Deutschlands e.V.
Deutsche Vereinigung für Datenschutz e.V.
Bitkom e.V.
davit – Arbeitsgemeinschaft IT-Recht im Deutschen Anwaltverein e.V.
eco – Verband der Internetwirtschaft e.V.
VAUNET – Verband Privater Medien e.V.
Stiftung Datenschutz
UNHCR Deutschland
Katholisches Büro in Berlin
Bevollmächtigte des Rates der EKD bei der Bundesrepublik Deutschland
Diakonisches Werk der EKD
Deutscher Caritasverband
Deutsches Rotes Kreuz
AWO Bundesverband e.V.
Flüchtlingsrat Berlin
Jesuitenflüchtlingsdienst Deutschland

Deutsches Institut für Menschenrechte
Bund Deutscher Verwaltungsrichter und Verwaltungsrichterinnen
PRO ASYL, Bundesweite Arbeitsgruppe für Flüchtlinge e. V.
Redaktionen der NJW, NStZ, NZWiSt, Beck Verlag, ZAP, AnwBl, DRiZ, FamRZ, FAZ, Süddeutsche Zeitung, Die Welt, taz, Handelsblatt, dpa, Spiegel, Focus, Deubner Verlag Online Recht, LTO, Beck aktuell, Jurion, Juris Nachrichten, Juve, LexisNexis Rechtsnews, Otto Schmidt Verlag, Kriminalpolitische Zeitschrift, Strafverteidiger Forum, Zeitschrift HRR Strafrecht, Der Paritätische, (NRV) NVwZ, ZAR, Asylmagazin, ANA, Informationsbrief Ausländerrecht, Datenschutzberater, Computer und Recht

Die Bundesrechtsanwaltskammer ist die Dachorganisation der anwaltlichen Selbstverwaltung. Sie vertritt die Interessen der 28 Rechtsanwaltskammern und damit der gesamten Anwaltschaft der Bundesrepublik Deutschland mit rund 166.000 Rechtsanwältinnen und Rechtsanwälten[1] gegenüber Behörden, Gerichten und Organisationen – auf nationaler, europäischer und internationaler Ebene.

Vorbemerkung

Mit dem am 12. März 2026 vom Bundesministerium der Justiz und für Verbraucherschutz (BMJV) vorgelegten Referentenentwurf eines Gesetzes zur Änderung der Strafprozessordnung – digitale Ermittlungsmaßnahmen (im Folgenden: RefE-Ermittlungsmaßnahmen) sollen zwei Rechtsgrundlagen für einen automatisierten Datenabgleich geschaffen werden. Beim automatisierten Datenabgleich soll auch sog. Künstliche Intelligenz zum Einsatz kommen dürfen,[2] sofern die eingesetzte Software im Einklang mit den Vorgaben der Verordnung (EU) 2024/1689 (KI-Verordnung) entwickelt und betrieben wird.[3]

Mit dem parallel vom Bundesministerium des Innern (BMI) am selben Tag vorgelegten Gesetzesentwurf zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit (im Folgenden: RefE-Polizeiarbeit) sowie zum Gesetzesentwurf zur Stärkung digitaler Ermittlungsbefugnisse zur Abwehr von Gefahren des internationalen Terrorismus (im Folgenden: RefE-Terrorismus) werden vergleichbare Regelungen vorgeschlagen.

Die vorliegende Stellungnahme richtet ihren Fokus auf die vorgeschlagene Einführung der strafprozessualen Vorschriften des Referentenentwurfes des BMJV zu digitalen Ermittlungsmaßnahmen (§§ 98d, 98e StPO-RefE-Ermittlungsmaßnahmen) und die damit einhergehenden Risiken. Ein Großteil der hierzu im Folgenden geäußerten Bedenken ist auf die vom BMI vorgeschlagenen Regelungen übertragbar. Auf diese wird daher nur vereinzelt gesondert eingegangen. Die Bundesrechtsanwaltskammer nimmt dankend wie folgt Stellung:

I. Änderungsvorschläge im Überblick

Mit den Gesetzentwürfen liegen Vorhaben vor, die in Ansätzen bereits in der vergangenen Legislaturperiode als BT-Drs. 20/12806 unter dem Namen „Sicherheitspakt“ diskutiert worden sind und letztlich dem Grundsatz der sachlichen Diskontinuität zum Opfer gefallen sind. Die nun zu bewertenden Vorhaben gehen in den, den Behörden in StPO, BKAG und BPolG sowie teilweise im AsylG eingeräumten, Befugnissen jedoch noch weiter.

Die erste Regelung soll den Behörden den **automatisierten Abgleich biometrischer Daten aus einem Strafverfahren mit öffentlich zugänglichen Daten aus dem Internet** erlauben (§ 98d StPO-RefE-Ermittlungsmaßnahmen sowie die damit korrespondierenden Parallelvorschriften in BKAG-RefE-Terrorismus, BPolG-RefE-Polizeiarbeit und AsylG-RefE-Polizeiarbeit). Sie soll damit unmittelbar der Gewinnung **neuer Erkenntnisse und Beweismittel** dienen. Es handelt sich insoweit um eine neue Open-Source-Intelligence-Maßnahme (OSINT-Maßnahme) zur Gewinnung von im Internet frei

[1] Im Interesse einer besseren Lesbarkeit wird nicht ausdrücklich in geschlechtsspezifischen Personenbezeichnungen differenziert. Die im Folgenden gewählte männliche Form schließt alle Geschlechter gleichberechtigt ein.

[2] Vgl. RefE-Ermittlungsmaßnahmen, S. 9. Zu den besonderen Risiken vgl. auch BVerfG, Urt. v. 16.2.2023 – 1 BvR 1547/19 u.a., Rn. 100.

[3] Vgl. RefE-Ermittlungsmaßnahmen, S. 10 f.

zugänglichen Daten.[4] Der Abgleich mit öffentlich-zugänglichen Echtzeitdaten[5] soll dabei unzulässig bleiben. Öffentlich zugänglich sind Daten, die von jedermann verwendet werden können, bspw. auch aus den sozialen Medien, soweit sich diese nicht an einen spezifisch abgegrenzten Personenkreis richten.[6] Dabei reicht es für die öffentliche Zugänglichkeit aus, wenn die Daten nach einer Registrierung[7]/Genehmigung/Entgeltzahlung genutzt werden können.

Die zweite Regelung sieht eine **Befugnis zur automatisierten verfahrensübergreifenden Datenanalyse** auf bereits anderweitig – strafprozessual oder gefahrenabwehrrechtlich – (legal) erhobene und von Polizeien gespeicherte Daten vor (**§ 98e StPO-RefE-Ermittlungsmaßnahmen**, BKAG-RefE-Terrorismus und BPolG-RefE-Polizeiarbeit). Insoweit soll die Maßnahme nicht der Erhebung neuer Beweismittel dienen, wohl aber dem Gewinn **neuer Erkenntnisse** auf Grundlage einer automatisierten Analyse bestehender Datenbestände. Die Rechtsgrundlage soll eine vom Bundesverfassungsgericht (BVerfG) aufgezeigte vermeintliche Regelungslücke schließen, nachdem das BVerfG festgestellt hatte, dass verfahrensübergreifende automatisierte Datenanalysen und -auswertungen nur auf Grundlage einer Ermächtigungsgrundlage in Betracht kommen.[8] Dabei geht es primär um die Analyse von Daten, die von den Polizeibehörden der Länder und des Bundes innerhalb ihrer Zuständigkeitsbereiche bereits für den Betrieb einer verfahrensübergreifenden Recherche- und Analyseplattform zur Gefahrenabwehr zusammengeführt wurden. Folge der neuen Ermächtigungsgrundlagen ist eine Zusammenführung (von präventiv **und** repressiv erhobenen Daten) in einer separaten Analyseplattform zur automatisierten Analyse, die auch KI-gestützt erfolgen darf.

II. Einleitung

Das im Grundsatz nachvollziehbare Bestreben des RefE Ermittlungsmaßnahmen ist es, Ermittlungsbehörden mit modernen Ermittlungsbefugnissen auszustatten, um ressourcenintensive manuelle Suchabfragen durch einen automatisierten Abgleich bzw. eine automatisierte Datenanalyse zu ersetzen oder zumindest zu ergänzen.[9] Ebenso erkennbar sind die im vorgeschlagenen Normtext und der Begründung vorgenommenen Einschränkungen, um die Grundrechtssensibilität der beiden Maßnahmen zu reduzieren.

Aus Sicht der Bundesrechtsanwaltskammer bestehen hingegen erhebliche Bedenken, ob die vorgeschlagenen Regelungen der besonderen Eingriffstiefe und der Streubreite der Maßnahme angemessen Rechnung tragen. Die Bundesrechtsanwaltskammer tritt deshalb den Gesetzesentwürfen entschieden entgegen. Insbesondere der bei solch weitgehenden Maßnahmen gebotene Grundrechtsausgleich ist nicht gelungen. Mit Blick auf die technische Umsetzung solcher Maßnahmen bestehen zudem praktische Bedenken.

Die Bundesrechtsanwaltskammer ruft in Erinnerung, was das BVerfG u. a. in diversen aktuellen Entscheidungen[10] betont hat: Wenn der Gesetzgeber eine Ermittlungsmaßnahme einführt, hat sich die

---

[4] Vgl. RefE-Ermittlungsmaßnahmen, S. 6.

[5] Insbesondere Live-Videos in den sozialen Medien; aufgezeichnete Videos sollen gleichwohl unter die Regelung fallen.

[6] BMJV, RefE-Ermittlungsmaßnahmen, 2026, S. 12.

[7] Z.B. Instagram oder andere soziale Medien, wenn Privatsphäre-Einstellungen den Zugriff auch ohne „Folgeanfrage“/„Freundschaft“ oder ähnliches erlauben.

[8] BVerfG, Urt. v. 16.2.2023 – 1 BvR 1547/19 u.a., NJW 2023, 1196.

[9] Vgl. RefE-Ermittlungsmaßnahmen, S. 15.

[10] BVerfG, Beschl. v. 24.06.2025 – 1 BvR 180/23, „Trojaner II“, Rn. 188; BVerfG, Urt. 16.02.2023 - 1 BvR 1547/19, 1 BvR 2634/20, "Automatisierte Datenanalyse" Rn. 149; BVerfG, Urt. v. 26.04.2022 - 1 BvR 1619/17, "Bayerisches Verfassungsschutzgesetz" Rn. 325 f.;

verfassungsrechtliche Bewertung an den von der Befugnis eröffneten rechtlichen und tatsächlichen Nutzungsmöglichkeiten zu orientieren.

Um eine Aushöhlung der Grundrechte auf informationelle Selbstbestimmung (Art. 1 Abs. 1 i. V. m. Art. 2 Abs. 1 GG), auf ungehinderte und unüberwachte Telekommunikation (Art. 10 Abs. 1 GG), auf unüberwachte Wohnung (Art. 13 Abs. 1 GG) und auf Eigentum (Art. 14 Abs. 1 GG) zu verhindern, müssen strafprozessuale Eingriffsnormen in digitale Daten

- hohe Eingriffsschwellen (bestimmte Tatsachengrundlage, bezogen auf einen konkreten Straftatenkatalog schwerer Straftaten) vorsehen,
- die Datenquellen und die Analysemethoden präzise bestimmen,
- die Zweckbindung der erhobenen Daten aufrechterhalten und durch geeignete Kennzeichnungen bekräftigen,
- den Richtervorbehalt und andere Anforderungen der Verhältnismäßigkeit beachten, sowie
- den Betroffenen uneingeschränkte Transparenz und effektiven Rechtschutz ermöglichen.[11]

Im Lichte dieser verfassungsgerichtlichen Vorgaben sind folgende Aspekte hervorzuheben:

- Die genauen technischen, organisatorischen und rechtlichen Rahmenbedingungen für den (avisierten) Einsatz von automatisierten Systemen sind noch weitgehend unbekannt. Es ist zum jetzigen Zeitpunkt unklar, über welche genauen Funktionalitäten die jeweilige Software verfügen wird, auf welche Datenbestände diese zugreifen wird und welche Einsatzszenarien im Fokus stehen sollen. Zwar lassen sich bestimmte Anwendungsfelder aufgrund von Erfahrungen im gefahrenabwehrrechtlichen Bereich sowie Presseberichten ausmachen. Allerdings liegt dem Referentenentwurf kein klar abgrenzbarer, transparent nachvollziehbarer und damit einer rechtlichen Bewertung zugänglicher Anwendungsfall zugrunde.

- Der Referentenentwurf definiert auch kein klares gesetzliches Leitbild für den Einsatz der jeweiligen Systeme. § 98d StPO-RefE-Ermittlungsmaßnahmen lässt den Einsatz zu *„[z]ur Erforschung des Sachverhalts, zur Identitätsfeststellung oder zur Ermittlung des Aufenthaltsorts des Beschuldigten oder eines Zeugen […].“* Die automatisierte Datenanalyse nach § 98e StPO-RefE-Ermittlungsmaßnahmen soll zulässig sein *„[z]ur Aufklärung der Straftat oder zur Ermittlung des Aufenthalts einer Person, nach der für die Zwecke des Strafverfahrens gefahndet wird […].*“ Als Datenquelle nennt § 98d StPO-RefE-Ermittlungsmaßnahmen das öffentlich zugängliche Internet und erfasst damit sowohl personenbezogene Daten des Beschuldigten als auch Daten von Zeugen oder vollständig unbeteiligten Personen.[12] Bei § 98e StPO-RefE-Ermittlungsmaßnahmen sollen als Datenquellen „*Vorgangsdaten, Falldaten, Daten aus den polizeilichen Informationssystemen und aus dem polizeilichen Informationsaustausch einbezogen werden*.“ Der Bundesgesetzgeber regelt indes nicht, wie Vorgangsdaten, Falldaten und weitere Daten zu erheben und die Datenbestände zu verwalten sind und räumt damit sowohl dem Landesgesetzgeber als auch der polizeilichen Praxis erhebliche Spielräume ein, den Datenbestand für die automatisierte Datenanalyse zu definieren.

Angesichts des Mangels an klar definierten bundesgesetzlichen Vorgaben für den Einsatz automatisierter Datenverarbeitung nach § 98d, § 98e StPO-RefE-Ermittlungsmaßnahmen bestehen durchgreifende **Bedenken**, ob die **verfahrensrechtlichen Hürden** (insbesondere hinsichtlich des Verzichts auf einen Richtervorbehalt) und **Eingriffsvoraussetzungen** (Beschränkung auf Straftaten von erheblicher

[11] BVerfG, Urteil vom 16.02.2023 - 1 BvR 1547/19, u. a., amtliche Leitsätze, u. a. Rn. 105 ff.; vgl. auch *Teichmann*, Automatisierte Datenanalyse im Gefahrenabwehrrecht, hrrs 01-2026, S. 13, 14.

[12] Vgl. zur besonderen Eingriffstiefe BVerfG, Urt. v. 16.2.2023 – 1 BvR 1547/19 u.a., Rn. 94.

Bedeutung bzw. den Straftatenkatalog des § 100a Abs. 2 StPO) ausreichend sind, um die damit einhergehenden Grundrechtseingriffe, insbesondere auch für Nichtbeschuldigte, zu rechtfertigen.

Im Zentrum der Entwurfsbegründung stehende Effizienz- und Effektivitätserwägungen vermögen die Erforderlichkeit und Angemessenheit der Maßnahmen für sich genommen nicht zu belegen.[13]

Die Bundesrechtsanwaltskammer mahnt an, beide Vorschriften im Lichte der folgenden, schlaglichtartig dargestellten Problemkonstellationen **auf ihre Verfassungskonformität hin zu überprüfen**. Es ergibt sich bei genauerer Prognose zumindest eine konkrete Wahrscheinlichkeit für äußerst intensive Eingriffe in die Grundrechte einer Vielzahl von Personen, die keineswegs gleichzeitig im gleichen Maß von dem Ermittlungsziel (Aufklärung einer Straftat) betroffen sein können. Die vorgeschlagenen Regelungen tragen Art und Umfang dieser Eingriffe nicht angemessen Rechnung. Darüber hinaus ergibt sich auch **punktueller Bedarf für Anpassungen**, die indes eine generelle Überprüfung der Regelungen aus Sicht der Bundesrechtsanwaltskammer nicht ersetzen können.

III. Automatisierter biometrischer Abgleich mit öffentlich zugänglichen Daten aus dem Internet, § 98 StPO-RefE-Ermittlungsmaßnahmen

Die Vorschrift des § 98d Abs. 1 StPO-RefE-Ermittlungsmaßnahmen erlaubt einen biometrischen Abgleich mit im Internet öffentlich zugänglichen Daten. Vom biometrischen Abgleich erfasst ist u. a. ein visueller Abgleich und ein Stimmabgleich. Unter einem biometrischen Abgleich im Sinne der Vorschrift ist die technisch gestützte Überprüfung der Übereinstimmung von biometrischen Signaturen mit dem Ergebnis einer Übereinstimmungsbewertung zu verstehen.[14]

Die Intensität des Eingriffs in das Recht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG über § 98d StPO-RefE-Ermittlungsmaßnahmen und dessen Parallelvorschriften in BKAG-RefE-Terrorismus und BPolG-RefE-Polizeiarbeit bzw. dem AsylG-RefE-Polizeiarbeit wird zuvorderst durch die Heimlichkeit der beabsichtigten (präventiven) Maßnahme und durch ihre Streubreite begründet.[15] Der Betroffene kann gegen solche Maßnahmen weder gerichtlichen Rechtsschutz vor ihrer Durchführung erlangen noch durch sein Verhalten den Gang der Maßnahmen beeinflussen.[16]

1. Keine Differenzierung zwischen Beschuldigten und Nichtbeschuldigten

Die Maßnahme erlaubt ausdrücklich auch den biometrischen Abgleich von biometrischen Signaturen eines **Nichtbeschuldigten**, z. B. eines Zeugen.[17] Durch eine nachträgliche Auswertung können ganze Bewegungsprofile erstellt und Personen vollständig durchleuchtet werden. Im – nicht völlig fernliegenden – Extremfall kann es sein, dass Betroffene selbst nicht über eigene Accounts z. B. auf sozialen Medien verfügen, aber ohne Unkenntlichmachung im Hintergrund auf dort hochgeladenen Bildern auftauchen. Dem Schutz unbeteiligter Personen durch einen solchen Eingriff wird indessen keine Rechnung getragen, da die vorhergesehenen Voraussetzungen des Eingriffs, anders als z. B. bei der Telekommunikationsüberwachung (§ 100a Abs. 3 StPO) oder der einfachen Durchsuchung (§§ 102, 103 Abs. 1 Satz 1 StPO), bei Beschuldigten und Nichtbeschuldigten identisch ausgestaltet werden sollen. Damit unterscheidet sich die vorgeschlagene Vorschrift auch von der Verkehrsdatenerhebung (§ 101a

---

[13] Siehe im Einzelnen: RefE-Ermittlungsmaßnahmen, S. 1: "*Dies kann [...] zur Erfolglosigkeit von Ermittlungsmaßnahmen führen und außerdem in erheblichem Umfang Personal der Strafverfolgungsbehörden binden*" *sowie auf S. 2: "Auf der anderen Seite ist von kostenrelevanten Effektivitätsgewinnen auszugehen*" und RefE-Polizeiarbeit, S. 17: "*Dies bindet zum einen personelle Ressourcen*".

[14] Vgl. RefE-Ermittlungsmaßnahmen, S. 12.

[15] *Rückert*, ZStW 2017, 302, 320 f.

[16] *Rückert*, ZStW 2017, 302, 320.

[17] Vgl. RefE-Ermittlungsmaßnahmen, S. 12; *Rückert*, ZStW 2017, 302, 320 f.

Abs. 1 StPO) sowie den Anwendungsfällen der §§ 100i Abs. 1, 100k Abs. 1 StPO (vgl. § 101a Abs. 1a StPO), obwohl der RefE-Ermittlungsmaßnahmen einen weitgehenden Gleichlauf mit diesen Regelungen intendiert.[18] Dieser intensive Eingriff wird auch nicht dadurch ausreichend abgemildert, dass der biometrische Internetabgleich nur subsidiär zulässig sein soll.[19]

Gerade aufgrund dieses intensiven Eingriffs **–** und zum Schutz vor etwaigem Missbrauch **–** müsste der in Bezug genommene **Straftatenkatalog** jedenfalls **abschließend** ausgestaltet sein.[20] § 98d Abs. 1 Nr. 1 StPO-RefE-Ermittlungsmaßnahmen und § 9a Abs. 2 BKAG-RefE-Polizeiarbeit verweisen zwar auch auf die Straftaten in § 100a Abs. 2 StPO. Jedoch reichen nach dem Wortlaut der Normen auch andere Straftaten von erheblicher Bedeutung aus. Darüber hinaus wurde schon im vergangenen Gesetzgebungsverfahren dieser (damals abschließende) Verweis von der Bundesdatenschutzbeauftragten kritisiert.[21] Der Straftatenkatalog des § 100a Abs. 2 StPO unterliege ständigen Erweiterungen und Neuregelungen, so dass er nicht geeignet sei, eine Maßnahme trennscharf auf schwere Taten zu beschränken. Eine Bezugnahme auf den Katalog der Bezugstaten in § 138 StGB sei eher geeignet, eine taugliche Abgrenzung mit Blick auf schwere Taten zu schaffen.[22] Besonders schwer wiegt nun, dass in § 98d Abs. 1 Nr. 1 StPO-RefE-Ermittlungsmaßnahmen und § 9a BKAG-RefE-Polizeiarbeit erneut der ungeeignete Verweis auch auf § 100a Abs. 2 StPO erfolgt, dieser Verweis aber jetzt nicht abschließend ist. § 58a BPolG-RefE-Terrorismus verweist in seinem Abs. 1 Nr. 2 und Nr. 3 zudem **nur insbesondere** auf Straftaten nach §§ 315, 315b, 316b und 316c StGB. Die §§ 315b, 316b StGB sind lediglich mit einer Höchststrafe von fünf Jahren bedroht und gehören damit zur **mittleren –** nicht zur schweren **– Kriminalität**.[23] Auch hier wäre der Verweis auf § 138 StGB konsequenter, da sonst dem schwerwiegenden Eingriff in das Grundrecht auf informationelle Selbstbestimmung nicht ausreichend Rechnung getragen wird.

Unbefriedigend ist auch die Anordnungsbefugnis in § 98d Abs. 4 StPO-RefE-Ermittlungsmaßnahmen ausgestaltet. Ein **Richtervorbehalt ist nicht vorgesehen.**[24] Dies stimmt zwar mit der Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 (KI-VO) überein. Hier wird lediglich eine Justizbehörde vorausgesetzt.[25] Es bildet die Eingriffsintensität aber nicht hinreichend ab. Insbesondere weil die Maßnahme auch den Zugriff auf Daten ermöglicht, die ohne Verantwortung der abgebildeten und betroffenen Person zu „öffentlichen“ Daten geworden sind (siehe oben).

---

[18] Vgl. RefE-Ermittlungsmaßnahmen, S. 12.

[19] *Suliak*, Anwaltschaft kritisiert Hubigs Geschenk für die Strafverfolger, lto.de v. 12.03.2026, https://www.lto.de/recht/hintergruende/h/bmjv-digitale-ermittlungsmassnahmen-bildabgleich-internet-datenanalyse-kritik-rav-dav (zuletzt abgerufen am 26.03.2026); BMJV, RefE Digitale Ermittlungsmaßnahmen, 2026, S. 12.

[20] So auch *Rückert*, ZStW 2017, 302, 332 und Stellungnahme der Bundesbeauftragen für Datenschutz v. 11.09.2024, S. 3, https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Stellungnahmen/2024/StgN_Terrorismusbek%C3%A4mpfung-Gesetz.pdf?__blob=publicationFile&v=3 (zuletzt abgerufen am 30.03.2026).

[21] Stellungnahme der Bundesbeauftragen für Datenschutz v. 11.09.2024, S. 3 ff., https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Stellungnahmen/2024/StgN_Terrorismusbek%C3%A4mpfung-Gesetz.pdf?__blob=publicationFile&v=3 (zuletzt abgerufen am 30.03.2026).

[22] Stellungnahme der Bundesbeauftragen für Datenschutz v. 11.09.2024, S. 3, https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Stellungnahmen/2024/StgN_Terrorismusbek%C3%A4mpfung-Gesetz.pdf?__blob=publicationFile&v=3 (zuletzt abgerufen am 30.03.2026).

[23] Stellungnahme der Bundesbeauftragen für Datenschutz v. 11.09.2024, S. 5 f., https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Stellungnahmen/2024/StgN_Terrorismusbek%C3%A4mpfung-Gesetz.pdf?__blob=publicationFile&v=3 (zuletzt abgerufen am 30.03.2026).

[24] So auch: *Rückert*, ZStW 2017, 302, 332.

[25] Das wäre mit der Anordnung durch die Staatsanwaltschaft auch gegeben, vgl. auch *Suliak*, Anwaltschaft kritisiert Hubigs Geschenk für die Strafverfolger, lto. Dev. 12.03.2026, https://www.lto.de/recht/hintergruende/h/bmjv-digitale-ermittlungsmassnahmen-bildabgleich-internet-datenanalyse-kritik-rav-dav (zuletzt abgerufen am 30.03.2026).

Ferner sieht Art. 13 Abs. 2 Richtlinie (EU) 2016/680, umgesetzt in § 56 Abs. 1 BDSG, die Möglichkeit vor, die datenverarbeitende Stelle gesetzlich zur **aktiven Benachrichtigung der betroffenen Personen zu verpflichten**. Der automatisierte biometrische Abgleich mit öffentlich zugänglichen Daten aus dem Internet dürfte – wie bereits dargestellt – regelmäßig ohne Kenntnis der betroffenen Personen erfolgen. Die Einführung einer aktiven Benachrichtigungspflicht könnte – insbesondere im Hinblick auf den intensiven Grundrechtseingriff – zu einer ausgewogeneren Regelung beitragen.[26]

2. Beschränkte Schulungspflichten

Der (Online-)Einsatz automatisierter biometrischer Erkennungs- und Datenanalyse-Systeme erfordert spezifische technische Kenntnisse über deren Funktionsweise, Möglichkeiten und Grenzen. Insbesondere beim Einsatz von KI-Systemen ist ein Verständnis für deren Fehleranfälligkeit, Diskriminierungsrisiken und das Phänomen der "Halluzinationen" (siehe dazu unten) unerlässlich.

Positiv ist zu vermerken, dass § 9b Abs. 6 S. 1 BKAG-RefE-Polizeiarbeit sowie die dessen Parallelvorschrift § 39b Abs. 6 S. 1 BKAG-RefE-Terrorismus für die **automatisierte Datenanalyse** eine Schulungspflicht **für Polizeibedienstete** vorsehen:[27] **Lücken** weisen die Entwürfe insoweit jedoch an folgenden Stellen auf:

Bezüglich des **biometrischen Internetabgleichs** nach § 98d StPO-RefE-Ermittlungsmaßnahmen, § 9a BKAG-RefE-Polizeiarbeit, § 39a BKAG-RefE-Polizeiarbeit sowie für (sonstige) **Ermittlungsbeamte der Staatsanwaltschaft** (§ 152 GVG), die nach § 98d Abs. 4 S. 2 StPO-RefE-Ermittlungsmaßnahmen bei Gefahr im Verzug den Abgleich anordnen dürfen, ist keine Schulungspflicht vorgesehen. Gerade beim biometrischen Abgleich ist die Kenntnis über Fehlerquoten, Diskriminierungsrisiken und die korrekte Verifizierung der Treffer jedoch unerlässlich.

Soweit ein Richtervorbehalt eingeführt wird – wie er von der Bundesrechtsanwaltskammer umfassend gefordert, derzeit jedoch nur für Auslandsübermittlungen vorgesehen ist – ist gleichermaßen eine **Schulung der entscheidenden Richter** über Umfang, Art und Weise der Verwendung und die möglichen Gefahren bei der Verwendung digitaler Rechercheprogramme erforderlich, um rechtssichere Entscheidungen im Einzelfall zu gewährleisten. Dies gilt umso mehr, als die Richter die Funktionsweise der eingesetzten KI-Systeme verstehen müssen, um die Voraussetzungen der Anordnung sachgerecht prüfen zu können. Eine solche fehlt ebenfalls.

Entsprechendes gilt für **Staatsanwälte**, die nach § 98d Abs. 4 S. 1 StPO-RefE-Ermittlungsmaßnahmen den biometrischen Abgleich anordnen oder nach § 98e StPO-RefE-Ermittlungsmaßnahmen automatisierte Datenanalysen durchführen lassen können.

Soweit die Einführung entsprechender Schulungspflichten etwa mit Blick auf Landesbeamte oder Richter für nicht realisierbar erachtet wird, sollte wenigstens auf Risiko-Sensibilisierungen und freiwillige Schulungsangebote hingewirkt werden.

---

[26] *Ogorek*, LTZ 2024, 274, 280.

[27] RefE-Terrorismus, S. 6: „*Das Bundeskriminalamt gewährleistet [...], dass das für die Durchführung der Maßnahme nach Absatz 1 eingesetzte Personal besonders geschult wird.*"

3. Risiko des „Dataminings“

Weiter eingriffsverschärfend wirkt, dass zur Vorbereitung des Abgleichs auch Daten aus dem Internet heruntergeladen werden dürfen. Der RefE-Ermittlungsmaßnahmen führt in der Begründung aus:

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

Hintergrund dieser (impliziten) Erlaubnis zur temporären Speicherung dürften (IT-sicherheits-)technische Gründe sein. So dürfte/könnte ein sicherer und effektiver Betrieb der Software erfordern, dass ein Datenabgleich mit sensiblen Verfahrensinhalten auf lokaler Ebene erfolgt.

Bei diesen (temporär) heruntergeladenen Daten handelt es sich denklogisch in weit überwiegendem Umfang um **personenbezogene Daten Unbeteiligter**. Denn vor einem Abgleich mit den biometrischen Daten der Zielperson wird, soll der automatisierte Abgleich einen praktischen Mehrwert gegenüber der manuellen Sichtung (z. B. des öffentlich zugänglichen Facebook-Profils des Beschuldigten) haben, eine breitflächige Analyse von Daten unbeteiligter Dritter erfolgen. Mit der (wohl technisch bedingten) Zulassung einer temporären Speicherung von Vergleichsdaten, wird dem „Datamining“ zum Zwecke des nachgelagerten Abgleichs die Tür geöffnet. Eine Begrenzung, welche Daten für einen solchen Abgleich heruntergeladen werden dürfen, sieht der RefE-Ermittlungsmaßnahmen nicht vor. Mit anderen Worten: Wenn von den jeweiligen Sachbearbeitern eine großflächige Suche nach der Zielperson für erforderlich erachtet wird, könnten Bilder und Videos von Tausenden oder gar Millionen unbeteiligter Bürger für die Zwecke des Abgleichs heruntergeladen werden. Doch auch bei einer fokussierten Suche gilt, dass die **Streubreite der Maßnahme enorm** ist. Dies wird nicht hinreichend kompensiert durch die auf die Durchführung der Maßnahme gerichtete Vorgabe einer temporären Speicherung der Daten ohne Kenntnisnahme durch Ermittlungsbeamte, da auch insoweit kein Zugriffsausschluss durch ein bindendes Berechtigungskonzept vorgegeben ist.

Darüber hinaus ist zu besorgen, dass für den Fall der Einführung des § 98d StPO-RefE-Ermittlungsmaßnahmen im Nachhinein ein erheblicher Reformdruck entstehen könnte, mit dem Ziel die Regelungen zur (temporären) Speicherung zu lockern. Denn unzweifelhaft ist das „Datamining“ im Einzelfall zum einen ressourcenintensiv und damit auch ökologisch wenig nachhaltig. Zum anderen soll § 98d StPO-RefE-Ermittlungsmaßnahmen auch der Aufenthaltsbestimmung des Beschuldigten dienen und auch in Eilfällen einsetzbar sein. Hinzukommt, dass erwartungsgemäß die eingesetzte Software auch im Bereich der Gefahrenabwehr Verwendung finden wird. Gerade in Eilfällen ist ein System, welches zunächst eine langwierige Datenaufbereitung erfordert, nur bedingt geeignet. Insoweit ist zu begrüßen, dass die Schaffung einer dauerhaften Datenbank ausdrücklich ausgeschlossen sein soll (vgl. § 98d Abs. 3 StPO-RefE-Ermittlungsmaßnahmen).[28]

[28] Vgl. RefE-Ermittlungsmaßnahmen, S. 13.

4. Scraping-Verbot der KI-Verordnung

Art. 5 Abs. 1 lit. e) der KI-VO verbietet "*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.*"

Die Referentenentwürfe setzen sich mit diesem Verbot nicht hinreichend auseinander. Die bloße Erwähnung in den Begründungen, dass die Vorgaben der KI-VO unmittelbar gölten, löst den Widerspruch nicht auf.[29] Wie die Bundesdatenschutzbeauftragte zur im Jahr 2025 geleakten Entwurfsversion ausgeführt hat, erscheint die Entwicklung eigener legaler technischer Lösungen zur biometrischen Gesichtserkennung ohne Scraping "*unter heutigen technischen Gegebenheiten unrealistisch*". Ob die in der Begründung zu § 98d StPO-RefE-Ermittlungsmaßnahmen vorgesehene Limitierung auf temporäre Speicherungen praktisch und wirtschaftlich umsetzbar ist und auf diese Weise Art. 5 Abs. 1 lit. e) der KI-VO genügt werden kann, erscheint zweifelhaft. Etablierte kommerzielle Angebote dürften im Regelfall ebenfalls auf entsprechenden Datenbanken basieren.

5. Einsatz von KI – menschliche Entscheidung

Der Referentenentwurf weist darauf hin, dass sich aus der KI-VO ergibt, dass sichergestellt werden müsse,

> „*dass die Strafverfolgungsbehörden keine Entscheidung ausschließlich auf der Grundlage der Ausgabe solcher Systeme zur nachträglichen biometrischen Fernidentifizierung treffen, aus der sich eine nachteilige Rechtsfolge für eine Person ergibt*."

Der RefE-Ermittlungsmaßnahmen verhält sich indes nicht zu der Frage, ob im Anwendungsbereich des § 98d StPO-RefE-Ermittlungsmaßnahmen auch ein entscheidungsersetzender Einsatz von KI-Systemen intendiert ist oder zumindest faktisch droht. Hierbei dürfte zwischen den Anwendungsszenarien zu differenzieren sein:

- Bei der **Bestimmung des Aufenthaltsorts** von Beschuldigten oder Zeugen dürfte das Risiko von „Entscheidungen" durch die KI, die mit einem Risiko für die Verfahrensrechte des Beschuldigten einhergehen, vergleichsweise gering sein. Trifft die KI eine „*false positive*"-Entscheidung, d. h. erkennt sie eine Person, die nur vermeintlich die Zielperson ist, unterliegt die Entscheidung über weitergehende Maßnahmen dem jeweiligen Ermittlungsbeamten. Dieser kann eine Korrektur vornehmen.[30] Bei einer „*false negative*"-Entscheidung, d. h. die KI erkennt die Zielperson nicht und zeigt daher keinen Suchtreffer an, drohen keine unmittelbaren Konsequenzen.

- Bei der **Erforschung des Sachverhalts** kann der Einsatz von KI indes durchaus weitergehende Konsequenzen haben. Erfolgt der KI-Einsatz z. B. zur Ermittlung noch unbekannter Personen, kann das Ergebnis des automatisierten Abgleichs Grundlage für schwerwiegende prozessuale Maßnahmen sein (z. B. Wohnungsdurchsuchung, Erlass eines Haftbefehls). Allerdings besteht hier für den Fall eines „*false positive*" eine mehrfache Korrekturmöglichkeit (Prüfung durch Ermittlungsbeamte, Richtervorbehalt). Weitergehende Auswirkungen dürften in der Praxis „*false negative*"-Ergebnisse eines KI-Einsatzes haben, d. h., wenn die KI wesentliche (entlastende) Erkenntnisse übersieht. Beispielsfälle könnten sein, Erkenntnisse zum

[29] RefE-Ermittlungsmaßnahmen, S. 10-11, RefE-Polizeiarbeit, S. 27.

[30] Zum Risiko des „*automation bias*" vgl. *Rückert,* StV 2025, 350 (355 f.); *Brodowski* in: Wörner u.a. (Hrsg.), Digitalisierung des Rechts, 2024, 125 (135 f.).

(abweichenden) Aufenthaltsort im tatrelevanten Zeitraum (Übersehen eines Alibis) oder der längerfristige Aufenthalt im Ausland bei der Bestimmung einer inländischen Steuerpflicht. Derartige „übersehenen" Erkenntnisse sind in der Praxis regelmäßig einer menschlichen Überprüfung im Einzelfall entzogen, so dass die Selektion der KI faktisch die menschliche Entscheidung (z. B. bei Erlass eines Durchsuchungsbeschlusses) ersetzt. Insoweit ist allerdings zu berücksichtigen, dass derartige Risiken auch beim manuellen Abgleich bestehen. Darüber hinaus kann der Betroffene zumindest im Nachhinein die – öffentlich zugänglichen – Entlastungsbeweise vortragen, um die Belastungen des Grundrechtseingriffs zu minimieren. Dennoch besteht in derartigen Fallkonstellationen das Risiko einer KI-gesteuerten Verdachtsgewinnung, die schwerwiegende Grundrechtseingriffe zur Folge haben kann.

Im vorangegangenen Gesetzgebungsvorhaben wurde darüber hinaus die **technische Umsetzung** solcher Maßnahmen unter Beachtung von DSGVO, JI-RL und KI-VO bezweifelt.[31] In erster Linie wird auf Probleme hinsichtlich der **technischen Zuverlässigkeit** (Falschidentifikation/Bias) und den möglicherweise **überschätzten Erwartungen** dieser Maßnahmen hingewiesen. Gerade diese Aspekte lassen auch **Zweifel an der Verhältnismäßigkeit** der Maßnahme aufkommen.

6. Löschungspflicht

Die Vorschrift des § 98d Abs. 3 StPO-RefE-Ermittlungsmaßnahmen soll folgende Löschungsroutine etablieren:

> *„Die beim Abgleich erhobenen und verarbeiteten Daten sind nach Durchführung des Abgleichs unverzüglich zu löschen, soweit sie keinen konkreten Ermittlungsansatz für das Verfahren aufweisen."*

In der Begründung heißt es ferner:

> *„Nach Absatz 3 dürfen ausschließlich Daten weiterverarbeitet werden, soweit sich auf Grundlage des Abgleichs aus ihnen ein konkreter Ermittlungsansatz ergibt. Die Weiterverarbeitung richtet sich im Weiteren nach den allgemeinen Regelungen zur Weiterverarbeitung nach der Strafprozessordnung. Alle anderen für die Durchführung des Abgleichs erhobenen und verwendeten Daten sind unverzüglich zu löschen."*[32]

Unstreitig ist, dass die Daten aus dem Internet nur zum Zwecke des Abgleichs verarbeitet werden dürfen und diese, wenn der Abgleich erfolglos blieb, zu löschen sind. Damit wird insbesondere sichergestellt, dass verfahrensirrelevante (personenbezogene) Daten unverzüglich gelöscht werden. Eine dauerhafte Datenbank soll ausgeschlossen werden.[33]

Unklar ist allerdings, wie mit Daten verfahren werden soll, bei denen der Abgleich erfolgreich war. Unstreitig sollen diese für die Verfolgung der Anlasstat zur Verfügung stehen. Sprachlich unklar ist hingegen, wie zu verfahren ist, wenn sich aus diesen zwar ein Ermittlungsansatz ergibt, dieser Ermittlungsansatz indes eine Straftat betrifft, die nicht die Anforderungen des § 98d Abs. 1 StPO-RefE-Ermittlungsmaßnahmen erfüllt (Zufallstreffer für Nicht-Katalogtaten). Anders als beispielsweise § 479 Abs. 2 Satz 2 StPO, der auf § 161 Abs. 3 StPO verweist, bleibt im RefE-Ermittlungsmaßnahmen unklar, was unter „*Ermittlungsansatz für das Verfahren*" zu verstehen ist. Auch die Gesetzesbegründung ist insoweit nicht

---

[31] Stellungnahme *Sorge* – Universität des Saarlandes v. 22.09.2024, S. 2 ff. https://www.uni-saarland.de/fileadmin/upload/lehrstuhl/sorge/Paper-Downloads/2024_Stellungnahme_Bundestag_Sicherheitspaket.pdf (zuletzt abgerufen am 30.03.2026).

[32] RefE-Ermittlungsmaßnahmen, S. 13.

[33] RefE-Ermittlungsmaßnahmen, S. 13.

eindeutig, da der Verweis auf die allgemeinen Regelungen zur Weiterverarbeitung auch die Behandlung der intendierten Treffer betreffen könnte.

Gerade aufgrund der enormen Streubreite der geplanten Maßnahme wäre sicherzustellen, dass Zufallsfunde zu den Zielpersonen nicht ohne Weiteres verwendet werden dürfen, sondern eine Zweckänderung nur nach den Vorgaben des § 161 Abs. 3 StPO[34] zulässig ist.

7. IT-Sicherheit und digitale Souveränität bei Privaten und Drittstaaten

Die Referentenentwürfe sind ausdrücklich "*technik- und produktneutral*" ausgestaltet.[35] Dies ermöglicht die Verwendung kommerzieller Anbieter wie Clearview AI oder PimEyes, die auf durch "Scraping" gewonnenen Datenbanken basieren. § 9a Abs. 6 BKAG-RefE-Polizeiarbeit sowie § 39a Abs. 6 BKAG-RefE-Terrorismus erlauben zudem ausdrücklich, "*den Abgleich durch eine öffentliche oder nichtöffentliche Stelle in einem Drittstaat durchführen [zu] lassen und hierzu an diese Stelle erforderliche Daten [zu] übermitteln*".[36]

Die Beauftragung einiger privater, insbesondere drittstaatlicher, Anbieter wirft jedoch Bedenken in Bezug auf die **Sicherheit und Kontrolle über die Datenverarbeitungen** auf. Angesichts der Eingriffstiefe sollte kritisch hinterfragt werden, inwieweit die Einhaltung von Grundrechtsgarantien sowie insbesondere der Anforderungen europäischer Datenschutz-, KI- und Digitalgesetze in diesen Fällen durch die beauftragenden Stellen garantiert werden kann. Sofern der Einsatz entsprechender Akteure im Ergebnis nicht ausgeschlossen wird, sollten zumindest weitergehende Schutzvorgaben erwogen werden, namentlich Zertifizierungspflichten, Ausschlusskriterien für Anbieter aus Hochrisiko-Staaten, verpflichtende Sicherheitsüberprüfungen, Anforderungen an Serverstandorte sowie Schutzvorkehrungen gegen Zugriffe ausländischer Geheimdienste. Insbesondere die in § 9a Abs. 6 BKAG-RefE-Polizeiarbeit sowie § 39a Abs. 6 BKAG-RefE-Terrorismus für das Bundeskriminalamt vorgesehene Möglichkeit, bei der Übermittlung an drittstaatliche Stellen von den Zweckbindungsgewährleistungen des § 81 Abs. 1 Nr. 3 und Abs. 4 BDSG abzusehen, öffnet der dauerhaften **zweckwidrigen Verwendung sensibelster Daten durch private Anbieter und ausländische Geheimdienste** Tür und Tor.

Die **Löschpflichten** in § 98d Abs. 3 StPO-RefE-Ermittlungsmaßnahmen und § 9a Abs. 4 BKAG-RefE-Polizeiarbeit gelten primär für die Behörden selbst. Bezüglich einiger privater ausländischer Anbieter wird teils bezweifelt, dass dorthin übermittelte Daten gelöscht werden oder dort dauerhaft in Trainingsdatenbanken verbleiben. Auch vor diesem Hintergrund sollte die Eröffnung entsprechender Übermittlungsbefugnisse hinterfragt werden – umso mehr, wenn dies in Kombination mit der vorgenannten Zweckbindungsausnahme geschieht.

8. Transparenzregelung des § 98d Abs. 2 StPO-RefE-Ermittlungsmaßnahmen

Die Vorschrift des § 98d Abs. 2 StPO-RefE-Ermittlungsmaßnahmen soll zwar Transparenz schaffen.[37] Aber der Grad einer solchen Transparenz durch die vorgeschlagene Regelung ist verschwindend gering. So ist zwar die „eingesetzte Software“ zu benennen. Da es sich hierbei allerdings um speziell für den polizeilichen Einsatz geschaffene Software handelt, die wiederrum auf Datenbestände zugreift, auf die nur die Polizei Zugriff hat, ist faktisch keine Transparenz über die angewandten Methoden, die ausgewerteten Quellen, sowie die letztlich erhobenen personenbezogenen Daten gegeben. Erforderlich

[34] Zur restriktiven Auslegung des § 161 Abs. 3 StPO vgl. BT-Drs. 19/4671, S. 64 mit Verweis auf BVerfG, Senatsurteil v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09; MüKoStPO/*Singelnstein*, 2. Aufl. 2024, StPO § 479 Rn. 33 ff.; *Hiéramente*, StV-S 2023, 45, 48.

[35] RefE-Terrorismus, S. 1; RefE-Polizeiarbeit, S. 2.

[36] RefE-Polizeiarbeit, S. 4-5.

[37] RefE-Ermittlungsmaßnahmen, S. 13.

wäre insoweit zumindest eine Pflicht, die im Einzelfall angeschlossenen Dateisysteme, d. h. die ausgewerteten Quellen sowie den Modus der Verifizierung der Daten durch solche Quellen, zu benennen, auf die die Software Zugriff genommen hat. Darüber hinaus sollte die grundsätzliche Funktionsweise der Software öffentlich zugänglich erläutert werden.[38]

IV. Automatisierte (verfahrensübergreifende) Datenanalyse, § 98e StPO-RefE-Ermittlungsmaßnahmen

Nach § 98e StPO-RefE-Ermittlungsmaßnahmen soll eine automatisierte Datenanalyse ermöglicht werden, die den Zugriff auf bereits legal erhobene und gespeicherte Daten ermöglichen soll. Nach der Vorstellung des Referentenentwurfs soll dabei sowohl ein Zugriff auf strafprozessual erhobene Daten als auch ein Zugriff auf nach dem Polizeirecht erhobene Daten ermöglicht werden.[39] Es bestehen angesichts der Weite der Vorschrift und der Unbestimmtheit der nutzbaren Daten erhebliche verfassungsrechtliche Bedenken. Ausgewählte Aspekte sollen im Folgenden beleuchtet werden.

1. Vermutung der rechtmäßigen Speicherung

Der Gesetzesentwurf stellt in § 98e Abs. 1 StPO-RefE-Ermittlungsmaßnahmen klar, dass in der automatisierten Datenanalyse nur „rechtmäßig gespeicherte“ Daten Verwendung finden dürfen. In der Begründung heißt es dazu:

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

Dieser bundesgesetzgeberische Appell ist nachvollziehbar und der Sache nach richtig. Der Referentenentwurf **verschließt hier allerdings die Augen vor den praktischen Realitäten** des Strafprozesses und des Gefahrenabwehrrechts.

Bereits im strafrechtlichen Ermittlungsverfahren kommt es, trotz staatsanwaltschaftlicher und ermittlungsrichterlicher Kontrolle, in der Praxis in steter Regelmäßigkeit zur (grob) rechtswidrigen Speicherung von Daten Beschuldigter, Zeugen und Unbeteiligter. Ein Paradefall ist die verbreitete staatsanwaltschaftliche Praxis, vorläufig sichergestellte Datenbestände auszuwerten und zur Akte zu nehmen,[40] oder die verbreitete Praxis, ganze Datenträger zu beschlagnahmen, obwohl die Verfahrensrelevanz der Daten noch nicht feststeht.

Darüber hinaus sehen die gesetzlichen Regelungen zwar eine Pflicht zur Löschung von verfahrensirrelevanten Daten, z. B. nach Zeitablauf, vor. Ausreichende Löschroutinen sind allerdings in der Praxis oftmals nicht oder nur halbherzig implementiert.

---

[38] Zu den Grenzen der Nachvollziehbarkeit von KI vgl. *Rückert,* GA 2023, 361 (366 f.); *Ahrens,* StraFo 2024, 242 (244).

[39] RefE-Ermittlungsmaßnahmen, S. 6, 15.

[40] Vgl. z.B. BVerfG, Beschl. v. 17.11.2022, 2 BvR 827/21; LG Hamburg, Beschl. v. 5.6.2025 . 616 Qs 14/25, Rn. 25: *„Wie das Amtsgericht in seinem Beschluss feststellt, geht diese fehlerhafte Sachbehandlung hochwahrscheinlich auf ein verbreitetes Fehlverständnis zurück, während eine bewusste und willkürlich fehlerhafte Sachbehandlung durch die Staatsanwaltschaft nicht zu erkennen ist.*“; *Park*, NStZ 2023, 646; *Hiéramente/Wagner*, StV-S 2023, 172.

Die rechtswidrige Speicherung von Daten betrifft darüber hinaus in der Praxis bedauerlicherweise wiederholt auch **Berufsgeheimnisträger**.[41] Stünden diese Daten im Rahmen einer automatisierten Datenauswertung zur Verfügung, würde der erhebliche (illegale) Eingriff in die Grundrechte des Berufsgeheimnisträgers sowie der Mandanten, Patienten, etc. perpetuiert und erheblich verstärkt. Der Bundesgesetzgeber will zwar ausschließen, dass illegal erlangte Daten in der Datenanalyse verwendet werden, kann dies allerdings nicht sicherstellen (vgl. dazu weiter unter IV. 3.).

Weitgehend unklar ist, in welchem Umfang sich gefahrenabwehrrechtlich tätige Polizeibehörden an die datenschutzrechtlichen Grundsätze, insbesondere den Grundsatz der Datensparsamkeit, halten und irrelevante Daten löschen. Diese Datenerhebung unterliegt in der Praxis auch nur einer eingeschränkten Kontrolle, da – anders als bei strafprozessualen Ermittlungsmaßnahmen – oftmals kein Korrektiv durch eine anwaltlich veranlasste gerichtliche Überprüfung besteht. Die gefahrenabwehrrechtliche Datenerhebung unterliegt damit weitgehend der Eigenkontrolle durch rechtlich nur bedingt geschulte Polizeibeamte. Es besteht daher ein erhebliches Risiko der weitgehend unkontrollierten Datenspeicherung.[42]

Darüber hinaus eröffnet der Referentenentwurf den Zugriff auf gefahrenabwehrrechtlich erhobene Daten, ohne eine inhaltliche Beschränkung auf konkrete Arten der Datenerhebung vorzunehmen. Im Kern handelt es sich dabei um eine **dynamische Verweisung auf landesrechtliche Vorschriften** in der jeweils geltenden Fassung. Eine Beschränkung auf Maßnahmen, die nach der StPO zulässig wären, sieht der Ref-Ermittlungsmaßnahmen nicht vorher.[43] Zwar lässt sich mittlerweile eine gewisse Angleichung der Regelungen zwischen Gefahrenabwehrrecht und Strafprozessrecht konstatieren. Dennoch überlässt es der Bundesgesetzgeber hier ganz bewusst dem Landesgesetzgeber, eigenständig die zulässigen Formen der Datenerhebung zu definieren, auf deren Grundlage die für die Datenanalyse zu verwendenden Daten gewonnen werden dürfen.[44]

Der Bundesgesetzgeber schafft mithin eine Regelung, die zwar vorgibt, die automatisierte Datenanalyse auf rechtmäßig gespeicherte Daten zu beschränken, ohne allerdings organisatorisch, technisch[45] oder rechtlich eine derartige Beschränkung durchsetzen zu können.

Der Bundesgesetzgeber hat zu definieren, welche Ermittlungsmaßnahmen er für zulässige Maßnahmen der Datenerhebung erachtet. Die **Bundesrechtsanwaltskammer fordert** insoweit, dass zumindest klargestellt wird, dass **nur Daten in die Datenanalyse einbezogen werden dürfen, die in einem strafrechtlichen Ermittlungsverfahren in zulässiger Weise hätten erhoben werden dürfen**.

2. Fortgeltung von Datenverarbeitungsvorgaben

Eng verwandt mit der soeben genannten Thematik ist die Problematik der Fortgeltung datenschutzrechtlicher Vorgaben. Der RefE-Ermittlungsmaßnahmen führt aus:

> *„Die für die speichernde Stelle geltenden gesetzlichen Vorgaben für die Verarbeitung personenbezogener Daten und die Rechte der Betroffenen einschließlich der geltenden Übermittlungsvorschriften und Verwendungsregelungen gelten dabei fort. Dies betrifft insbesondere auch die Speicher-*

[41] Vgl. z.B. BVerfG, Beschl. v. 21.7.2025 – 1 BvR 398/24; LG Hamburg, Beschl. v. 20.1.2023 – 608 Qs 12/22; Saarländisches Anwaltsblatt 2025, S. 6 ff.

[42] Vgl. zum Zugriff auf „heimlich" erlangte Daten auch BVerfG, Urt. v. 16.2.2023 – 1 BvR 1547/19 u.a., Rn. 76.

[43] Vgl. zur Beschränkung der Eingriffstiefe durch Beschränkung auf konkrete Maßnahmen BVerfG, Urt. v. 16.2.2023 – 1 BvR 1547/19 u. a., Rn. 82.

[44] Zur Problematik unzureichender Bestimmung des Datenbestandes durch den Gesetzgeber vgl. BVerfG, Urt. v. 16.2.2023 – 1 BvR 1547/19 u. a., Rn. 78.

[45] Vgl. dazu BVerfG, Urt. v. 16.2.2023 – 1 BvR 1547/19 u.a., Rn. 139.

und Löschfristen, die Kennzeichnungspflichten und etwaige Vorgaben zu Rollen- und Rechtekonzepten. Diese gelten in derselben Weise für die Daten nach deren Zusammenführung und sind daher zwingend technisch in das System zu implementieren, soweit hierzu in der jeweiligen polizeirechtlichen Ermächtigungsgrundlage keine besonderen Regelungen getroffen worden sind […].“[46]

Auch dies setzt allerdings voraus, dass die in den polizeilichen Datenbanken gespeicherten Daten ausreichend (technisch) gekennzeichnet sind.[47] Dies dürfte in der Praxis gerade bei Fallakten und Vorgangsdaten oftmals nur äußerst unzureichend der Fall sein. Denn insbesondere die Vorgangsdaten umfassen nach der Konzeption des Referentenentwurfs eine Vielzahl von Daten:

„Vorgangsdaten sind sämtliche Daten, die im Zusammenhang mit einer polizeilichen Tätigkeit bei einem bestimmten Einsatzanlass zu Personen und Sachen im polizeilichen Vorgangsbearbeitungssystem erfasst werden. Aufgenommen werden insbesondere Anzeigen, Ermittlungsberichte und Vermerke, die nicht nur Daten zu Verdächtigen, Beschuldigten oder sonstigen Anlasspersonen enthalten, sondern beispielsweise auch zu Personen, die Anzeige erstatten, Hinweise geben oder Zeuginnen oder Zeugen sind.“[48]

Auch hier gibt der RefE-Ermittlungsmaßnahmen zwar das Ziel vor, kann die Einhaltung dieser Vorgaben indes nicht sicherstellen. So kann auch hier der strafprozessuale Anwender nicht sicherstellen, ob der Speichernde die bestehenden Vorgaben einhält. Zudem kann der Bundesgesetzgeber nicht effektiv sicherstellen, dass der Landesgesetzgeber ausreichende gesetzliche Vorkehrungen trifft. Dies ist insbesondere auch deshalb bedenklich, weil in den polizeilichen Datenbanken u. a. auch Daten gespeichert sein können, die ursprünglich mit nachrichtendienstlichen Mittel erhoben wurden.[49]

3. Einschränkungen bei Daten aus eingriffsintensiven Maßnahmen

Es ist grundsätzlich zu begrüßen, dass der RefE-Ermittlungsmaßnahmen die Einbeziehung von Daten aus eingriffsintensiven Maßnahmen beschränken will. Allerdings ist die vorgeschlagene Hürde des § 98e Abs. 2 Satz 2 StPO-RefE-Ermittlungsmaßnahmen zu unbestimmt. Zwar soll hierfür eine gesonderte Begründungspflicht gelten, vgl. § 98e Abs. 5 Satz 1 StPO-RefE-Ermittlungsmaßnahmen. Allerdings dürfte die reine Erforderlichkeitsprüfung keine signifikante praktische Hürde darstellen. Insoweit ist auch nicht ausreichend, dass der RefE-Ermittlungsmaßnahmen in der Begründung ausführt:

„Diese Daten dürfen in die Analyse ergänzend einbezogen werden, soweit dies erforderlich ist. Dies ist der Fall, wenn die Daten für die Zwecke des konkreten Verfahrens benötigt werden, und wenn bereits vor Kenntnis vom Inhalt der Daten tatsächliche Anhaltspunkte dafür vorliegen, dass die einzubeziehenden Daten in Verbindung zum konkreten Suchanlass stehen könnten […]“[50]

Das Bundesverfassungsgericht stellte bereits 2023 fest, dass in das Grundrecht auf informationelle Selbstbestimmung nach Art. 2 Abs. 1 i. V. m Art. 1 Abs. 1 GG aller Betroffenen eingegriffen wird,[51] wenn eine automatisierte Anwendung zur Datenanalyse gespeicherte Datenbestände verarbeitet.

Ein solcher Eingriff liegt also bei den beabsichtigten Normen zur automatisierten Datenanalyse in der StPO, dem BKAG und dem BPolG auf der Hand. Wie schon im letzten Gesetzgebungsverfahren kritisch vorgebracht, werden auf Grundlage der beabsichtigten Normen dauerhafte und vor allem

[46] RefE-Ermittlungsmaßnahmen, S. 15.
[47] Vgl. BVerfG, Urt. v. 16.2.2023 – 1 BvR 1547/19 u. a., Rn. 65.
[48] RefE-Ermittlungsmaßnahmen, S. 16.
[49] Vgl. BVerfG, Urt. v. 16.2.2023 – 1 BvR 1547/19 u. a., Rn. 79.
[50] RefE-Ermittlungsmaßnahmen, S. 17.
[51] BVerfG, Urt. v. 16.2.2023 – 1 BvR 1547/19 u. a., NJW 2023, 1196.

einzelfallunabhängige **„Superdatenbanken“ des BKA und der Polizei** möglich gemacht.[52] Über § 98e StPO-RefE-Ermittlungsmaßnahmen dürfte auf die Datenbank der Polizei auch zugegriffen und diese zusammengeführten Daten weiterverarbeitet werden. Dies soll alle gespeicherten, personenbezogenen Daten betreffen, unabhängig davon, ob sie zur Gefahrenabwehr oder zur Strafverfolgung erhoben worden sind.[53] Diese Datenbank würde eine **Vielzahl von Daten Beschuldigter, Opfer, Zeugen oder sogar gänzlich unbeteiligter Personen** umfassen. Betroffen wären auch **extrem sensible Daten**, wie medizinische Gutachten, Adressen und Namen von Vergewaltigungsopfern und Angaben zu Details solcher Taten.[54] Daten unaufgeklärter Straftaten würden erst dann aus der Datenbank genommen werden, wenn diese verjährt sind, sodass der Rückzug auf eine bloß „temporäre Speicherung“ der Daten ausgehöhlt wird.

Ermöglicht die automatisierte Datenanalyse oder -auswertung einen so schwerwiegenden Eingriff in die informationelle Selbstbestimmung, ist dies nur unter engen Voraussetzungen zu rechtfertigen.[55] Die **vorgesehenen Einschränkungen in den jeweiligen Normen reichen dafür nicht aus**. Insbesondere verweisen § 98e Abs. 1 StPO-RefE-Ermittlungsmaßnahmen und § 9b Abs. 1 BKAG-RefE-Polizeiarbeit erneut auf § 100a Abs. 2 StPO (zur Kritik bzgl. Dieses Verweises siehe oben). Weil die beabsichtigten Maßnahmen gerade nicht trennscharf auf schwere Taten beschränkt werden, können die vorgesehenen Einschränkungen des Zugriffs, insbesondere über § 98 Abs. 2, Abs. 3 StPO-RefE-Ermittlungsmaßnahmen und die Pflicht zur Protokollierung der Begründung des Einsatzes der Maßnahme in Abs. 5 dieses Versäumnis nicht ausgleichen. Wiederum fehlt die Normierung eines Richtervorbehalts. Die Einschränkungen in § 9b Abs. 3, Abs. 5 und Abs. 6, § 58b Abs. 1 Nr. 2 und Nr. 3 BPolG-RefE-Polizeiarbeit bzw. -Terrorismus verweisen zudem ebenfalls auf die Straftaten nach den §§ 315, 315b, 316b und 316c StGB (zur Kritik bzgl. Dieses Verweises siehe oben).

Aufgrund der schwerwiegenden Eingriffe in die Grundrechte des Einzelnen ist folglich zumindest im Anwendungsbereich des § 98e Abs. 2 Satz 2 StPO-RefE-Ermittlungsmaßnahmen ein Richtervorbehalt analog den Regelungen zur Ersterhebung einzuführen.

Bedenklich ist die Regelung des § 98e Abs. 2 Satz 2 StPO-RefE-Ermittlungsmaßnahmen zudem aus einem weiteren Grund. Die Vorgaben bei einer strafprozessual begründeten Ersterhebung schreiben vor, dass sich derart eingriffsintensive Maßnahmen nur gegen Beschuldigte und ausgewählte Dritte richten dürfen. Der Tatbestand des § 98e Abs. 1 i. V. m. Abs. 2 Satz 2 StPO-RefE-Ermittlungsmaßnahmen soll hingegen den Zugriff auf diese Daten auch dann ermöglichen, wenn sich die neuen Ermittlungen gegen andere Beschuldigte richten.[56] In einem solchen Fall müsste der Datenzugriff bereits nach den Vorschriften der Ursprungserhebung zu prüfen sein, so dass für eine Folgeverwertung keine niedrigeren Anforderungen gelten können. Alternativ müsste der Zugriff auf Datenbestände beschränkt sein, die dem aktuellen Beschuldigten oder einem Nachrichtenmittler zugeordnet werden können.

Anpassungsbedarf besteht darüber hinaus bei der Regelung des § 98e Abs. 2 Satz 3 StPO-RefE-Ermittlungsmaßnahmen. Der Gesetzgeber nimmt hier bewusst Daten aus den eingriffsintensivsten Maßnahmen (§§ 100b, 100c StPO) aus der automatischen Datenanalyse heraus. Diese Entscheidung ist zu begrüßen, bedarf allerdings nach der Entscheidung des Bundesverfassungsgerichts in Sachen

---

[52] Stellungnahme der Bundesbeauftragen für Datenschutz v. 11.09.2024, S. 7, https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Stellungnahmen/2024/StgN_Terrorismusbek%C3%A4mpfung-Gesetz.pdf?__blob=publicationFile&v=3 (zuletzt abgerufen am 30.03.2026).

[53] BMJV, RefE Digitale Ermittlungsmaßnahmen, 2026, S. 15.

[54] Vgl. Stellungnahme der Bundesbeauftragen für Datenschutz v. 11.09.2024, S. 7 f. ff., https://www.bfdi.bund.de/SharedDocs/Downloads/DE/DokumenteBfDI/Stellungnahmen/2024/StgN_Terrorismusbek%C3%A4mpfung-Gesetz.pdf?__blob=publicationFile&v=3 (zuletzt abgerufen am 30.03.2026).

[55] BVerfG, Urt. v. 16.2.2023 – 1 BvR 1547/19 u.a., NJW 2023, 1196.

[56] Vgl. zur Thematik auch BVerfG, Urt. v. 16.2.2023 – 1 BvR 1547/19 u. a., Rn. 84.

„Trojaner II“ der **Ausweitung auf die Quellen-TKÜ** mittels Zugriffs auf informationstechnische Systeme.[57]

Weiterer **Anpassungsbedarf** besteht im Hinblick auf Daten, die mittels einer gegen **Berufsgeheimnisträger** gerichteten Maßnahme erlangt wurden. Diese Daten dürfen grundsätzlich nicht in die Datenanalyse einbezogen werden, um das Risiko der Perpetuierung illegaler Zugriffe auf privilegierte Daten zu minimieren (siehe oben unter IV. 1.). Darüber hinaus besteht bei Zugriffen auf privilegierte Datenbestände (z. B. Server, Computer, Mobilgeräte oder E-Mail-Accounts von Verteidigern und Rechtsanwaltskanzleien) eine konkrete Wahrscheinlichkeit dafür, dass dabei auch zu schützende Daten anderer Mandanten gesichert werden, die im Ausgangsverfahren möglicherweise nicht im Fokus stehen, im Rahmen einer Suche nach § 98e Abs. 1 StPO-RefE-Ermittlungsmaßnahmen allerdings gezielt herausgefiltert werden könnten. Eine Einbeziehung derartiger Daten in die Datenanalyse sollte, wenn überhaupt, nur unter erheblichen materiellen und prozessualen Schranken zulässig sein.

4. KI-Einsatz

Im Rahmen des § 98e StPO-RefE-Ermittlungsmaßnamen soll der Einsatz von KI ausdrücklich zugelassen sein:

> *„Der Einsatz künstlicher Intelligenz ist in den Grenzen der von der Ermächtigungsgrundlage vorgegebenen Auswertemethoden möglich und kann damit für sämtliche in Absatz 4 beschriebenen Anwendungsfälle genutzt werden. Insbesondere kann der Einsatz künstlicher Intelligenz dazu dienen, die technischen Möglichkeiten zu verbessern und im Rahmen des Datenabgleichs Ähnlichkeiten in Sachverhalten zu erkennen (beispielsweise beim modus operandi oder bei Organisationsstrukturen).“*[58]

Zugleich heißt es im vorgeschlagenen Gesetzestext:

> *„Die Methodik der automatisierten Anwendung zur Datenverarbeitung hat sich darauf zu beschränken, Daten aufzubereiten und bereitzustellen, die es den Strafverfolgungsbehörden ermöglichen, eigene Bewertungen und Entscheidungen zu treffen. Jeder Einsatz der Anwendung muss anlassbezogen und manuell ausgelöst werden und anhand von Suchbegriffen erfolgen, die sich aus einem konkreten Sachverhalt ergeben. Eine ausschließlich auf der Maßnahme nach Absatz 1 beruhende automatisierte Entscheidungsfindung, die unmittelbar eine nachteilige Rechtsfolge für die betroffene Person hat oder diese erheblich beeinträchtigt, ist unzulässig*.“[59]

Der Gesetzgeber untersagt mithin eine „unmittelbare“ automatisierte Entscheidungsfindung. Dabei blendet der Referentenentwurf allerdings aus, dass beim Einsatz einer fortgeschrittenen KI „faktisch“ eine reine automatisierte Entscheidung drohen kann. Wird eine „KI“ mit der Durchsicht erheblicher Datenbestände beauftragt, dürften die „Treffer“ der KI im Regelfall einer menschlichen Prüfung unterliegen. Ob die „KI“ allerdings aus der Vielzahl der Dokumente, eine „richtige“ Auswahl vornimmt und dem Ermittlungsbeamten damit ein zutreffendes Bild der Fakten- und Beweislage vermittelt, kann der Ermittlungsbeamte indes, will er den Suchlauf nicht selbstständig vornehmen, nicht kontrollieren. Allein die Selektion der Erkenntnisse kann die Entscheidungsgrundlage schaffen, die eine polizeiliche, staatsanwaltschaftliche und ermittlungsrichterliche Entscheidung weitgehend determiniert.

---

[57] Vgl. ausführlich BVerfG, Beschl. v. 24.6.2025 – 1 BvR 180/23, Rn. 201 ff.
[58] RefE-Ermittlungsmaßnahmen, S. 19.
[59] § 98e Abs. 4 Satz 2 StPO-RefE-Ermittlungsmaßnahmen.

Der Einsatz von „KI“ weist daher, insbesondere perspektivisch, eine erhebliche Eingriffstiefe auf, weil eine große Masse von Daten zu Beschuldigten, Zeugen und Unbeteiligten selektiert und auf diese Weise eine Entscheidung prädeterminiert wird. Insoweit bestehen erhebliche Bedenken, ob ein solcher Einsatz bei den vorgesehenen Anordnungsvoraussetzungen verfassungskonform ist.

Darüber hinaus besteht beim Einsatz von „KI“ ein erhöhtes Gefahrenpotential für gesetzlich privilegierte Vertrauensbeziehungen (§ 53 StPO). Neben dem Risiko des Zugriffs auf privilegierte Daten (vgl. bereits unter IV. 1. und 3.), besteht insoweit auch das Risiko, dass Beziehungen zu (nicht-beschuldigten) Berufsgeheimnisträgern für sich genommen als Suchkriterium verwendet werden. So könnte die „KI“ bestimmte Personen deshalb in den Fokus der Ermittler rücken, weil diese z. B. einen bestimmten Anwalt/Strafverteidiger (z. B. einen Experten für steuerliche Selbstanzeigen oder einen Experten im Bereich Sexualdelikte) konsultiert haben.[60] Insoweit besteht zumindest **Anpassungsbedarf** in § 98e Abs. 4 StPO-RefE-Ermittlungsmaßnahmen um sicherzustellen, dass die nach §§ 53, 97, 100d, 160a StPO privilegierte Beziehung des Berufsgeheimnisträgers zum Mandaten, Patienten, etc. als Kriterium technisch ausgeschlossen wird.

In den Entwurfsbegründungen zu § 9b Abs. 6 BKAG-RefE-Polizeiarbeit sowie zu § 98d und § 98e StPO-RefE-Ermittlungsmaßnahmen wird auf die unmittelbare Geltung der KI-VO verwiesen und der dort angeordnete Grundrechtsschutz damit offenbar für weitgehend gewährleistet erachtet. Auch insoweit sollte jedoch hinterfragt werden, ob und inwieweit diese Anforderungen in der Praxis tatsächlich umgesetzt werden (können). Es sollten konkretere Vorgaben in Betracht gezogen werden, mit denen dies unter Umständen besser gewährleistet und die ihrerseits für eine differenziertere Beurteilung der Verhältnismäßigkeit herangezogen könnten. Dies gilt umso mehr als derzeit ein Rückbau der KI-VO diskutiert wird.

Bedenken hinsichtlich der Gewährleistung eines hinreichenden Grundrechtsschutzes ergeben sich auch aus der technischen Funktionsweise von KI-Modellen. Deren Opazität erschwert nicht nur das Erkennen von fehlerhaft hergestellten Zusammenhängen oder „halluzinierten“ Ausgaben, sondern auch von Diskriminierungen, die gemäß § 9b Abs. 5 Satz 1 BKAG-RefE-Polizeiarbeit ausgeschlossen werden sollen. Eine fehlende Nachvollziehbarkeit des Ursprungs erlangter Daten oder neu erzeugter Informationen könnte in der Praxis ferner Verteidigerrechte beschränken.

5. Insbesondere: Erzeugung neuen Wissens

Die Begründung zu § 9b BKAG-RefE-Polizeiarbeit führt aus, dass sich automatisierte Datenanalysen dadurch auszeichnen, dass sie "*darauf gerichtet sind, neues Wissen zu erzeugen (BVerfG, a.a.O., Randnummer 67)*".[61] § 98e Abs. 4 Nr. 1 StPO-RefE-Ermittlungsmaßnahmen postuliert ferner, dass "*datei- und informationssystemübergreifend Beziehungen oder Zusammenhänge zwischen Verfahren, Vorgängen, Personen, Personengruppierungen, Institutionen, Organisationen, Objekten und Sachen identifiziert und hergestellt, sowohl qualitativ als auch quantitativ klassifiziert, strukturell analysiert und visualisiert werden*" können. Die Software soll also nicht nur vorhandene Informationen zusammenführen, sondern **neue Zusammenhänge herstellen**, die aus den Einzeldaten nicht ersichtlich sind und ausweislich der § 98e Abs. 4 Nr. 1 StPO-RefE-Ermittlungsmaßnahmen getroffenen Formulierung nicht rein ortsbezogen, sondern insbesondere in Bezug auf „Personen“ bzw. „Personengruppen“ erfolgen dürften. Dies ist in mehrerlei Hinsicht problematisch:

---

[60] Vgl. zu verfassungsrechtlichen Restriktionen bei Ermittlungsmaßnahmen zu Lasten von unverdächtigen Mandaten auf Grundlage eines strukturell ähnlichen Beratungsverhältnisses BVerfG, Beschl. v. 18.3.2009 – 2 BvR 1036/08, Rn. 68.

[61] RefE-Polizeiarbeit, S. 24

Zunächst deuten die Formulierungen auf Methoden hin, die charakteristisch für **personenbezogenes Predictive Policing**-Ansätze sind, mit denen nicht nur rückblickend, sondern auch künftige (vermeintliche) Straftaten vorhergesagt werden sollen, wodurch massiv in Persönlichkeitsgrundrechte eingegriffen würde.

KI-Systeme können Korrelationen erkennen, die keine kausalen Zusammenhänge widerspiegeln. Ohne menschliche Überprüfungsmöglichkeit können solche **Scheinkorrelationen** zu Fehlermittlungen führen (siehe bereits oben VI. 4.).

Die hergestellten **Zusammenhänge** dürften der zweckmäßigen Funktionsweise von KI-Modellen **weitgehend intransparent** bleiben. So dürfte kaum nachvollziehbar sein, nach welchen Kriterien die Software Zusammenhänge "herstellt" (siehe bereits oben III. 8. zu § 98d Abs. 2 StPO-RefE-Ermittlungsmaßnahmen). Eine Differenzierung von bloßen Koinzidenzen einerseits zu kausalen Verknüpfungen andererseits muss genau so wie die genutzten statistischen Methoden, nach denen Zusammenhänge als relevant eingestuft werden, zur Wahrung der Verteidiger- bzw. Betroffenenrechte sowie zwecks Umsetzung bestehender gesetzlicher Transparenzanforderungen nachvollziehbar bleiben. Dies wird in den vorgelegten Entwürfen nicht hinreichend sichergestellt.

Es entstünde insgesamt ein erheblicher **Überwachungsdruck** für eine unüberschaubar hohe Zahl von Betroffenen, die jederzeit damit rechnen müssten, aufgrund eines wie auch immer „erkannten“ Zusammenhangs Gegenstand von Ermittlungs- oder Präventionsmaßnahmen zu werden (siehe zum Betroffenenumfang bereits oben III. 3.). Dies gilt insbesondere für Personen, zu denen mit erhöhter Wahrscheinlichkeit Informationen in den betroffenen Datenbeständen zu finden sind – u. a. Rechtsanwälte (siehe dazu bereits oben IV. 4.).

Diese **Risiken** sollten zumindest durch **klarstellende Begrenzungen** der zulässigen Analysemethoden minimiert werden. Insbesondere sollte explizit ausgeschlossen werden, dass rein statistische Korrelationen ohne nachvollziehbare kausale Verknüpfung als Ermittlungsansatz dienen, dass Predictive Policing-Methoden zur Vorhersage künftiger Straftaten eingesetzt werden und dass die "Erzeugung neuen Wissens" ohne nachvollziehbare Dokumentation der Analyseschritte erfolgt (siehe zu letzterem bereits die Vorschläge oben unter III. 8 zu § 98d Abs. 2 StPO-RefE-Ermittlungsmaßnahmen).

6. Umgang mit KI-bedingten Schäden

Da falsch erzielte Ermittlungsergebnisse (z. B. durch Halluzinationen, falsch-positive biometrische Treffer, fehlerhafte Profilbildung) zu weiteren staatlichen Verfolgungshandlungen führen können (Durchsuchungen, Festnahmen, Untersuchungshaft), sind grundsätzlich ersatzfähige Schäden unbeteiligter oder zu Unrecht verdächtigter Personen absehbar. Jedoch ist bei KI-Fehlern die **Kausalität zwischen dem KI-Fehler und dem Schaden sowie ein Verschulden der handelnden Beamten nur schwer nachweisbar**, insbesondere wenn die Funktionsweise der KI intransparent ist (Black Box), mehrere Personen an der Entscheidungskette beteiligt waren, der Fehler in der Software selbst lag (z. B. Halluzination, Bias) oder die handelnden Beamten die Fehlerhaftigkeit nicht erkennen konnten. Die Referentenentwürfe enthalten keine spezifische Haftungsregelung für Schäden, die durch fehlerhafte KI-Ergebnisse entstehen. Es gelten lediglich die allgemeinen Regelungen zur Staatshaftung (Art. 34 GG, § 839 BGB) und strafprozessuale Entschädigungsregelungen (§§ 7 ff. StrEG), die der Zurechnungsproblematik keine Rechnung tragen. Sofern Zurechnungsaspekte, wie nach derzeitigem Entwurfsstand, nicht durch spezifische Haftungs-, Beweis- und Dokumentationsregeln ausgeglichen werden können, müssen sie wenigstens im Rahmen der Verhältnismäßigkeitsprüfung berücksichtigt werden.

7. Fehlende spezialisierte Kontrolle

Die Referentenentwürfe verweisen auf die allgemeine datenschutzrechtliche Kontrolle durch die zuständigen Datenschutzbeauftragten und Aufsichtsbehörden.[62] Eine spezialisierte Kontrolle für den Einsatz automatisierter Systeme und KI im neu vorgesehenen Befugnisrahmen sehen die Gesetzentwürfe indes nicht vor. Inwieweit eine solch allgemeine Datenschutzkontrolle ausreicht, sollte angesichts der erheblichen Eingriffsintensitäten hinterfragt werden. Insoweit sollte eine **Festschreibung spezifischer Kontrollbefugnisse** erwogen werden, namentlich eine verpflichtende ex-ante-Kontrolle während der Entwicklung und Implementierung, spezifische Zugangs- und Anordnungskompetenzen der Aufsichtsbehörde, eine verpflichtende unabhängige technische Überprüfung der Software vor ihrem Einsatz, regelmäßigen Qualitätskontrollen der KI-Ergebnisse und eine Governance ähnlich den aktuellen Anforderungen der KI-VO, eine verpflichtende Fehleranalyse insbesondere bei falsch-positiven Treffern, öffentliche Statistiken über Einsatz und Erfolg der Maßnahmen und eine Suspendierungsmöglichkeit bei zu hohen Fehlerquoten oder Diskriminierung.

8. Fakultativer Ausschluss von verfahrensirrelevanten Daten

Unklar ist, warum in § 98e Abs. 4 Nr. 2 StPO-RefE-Ermittlungsmaßnahmen ein fakultativer Ausschluss verfahrensirrelevanter Daten vorgesehen ist. Insoweit sollte klargestellt werden, dass verfahrensirrelevante Daten, sobald die fehlende Verfahrensrelevanz festgestellt wurde, auszuschließen und zu löschen sind.

* * *

[62] RefE-Ermittlungsmaßnahmen, S. 10; RefE-Polizeiarbeit, S. 27.