

Gesichtserkennung zwischen INPOL und Internet

Zur Zulässigkeit retrograder biometrischer Fernidentifizierung im Strafverfahren

von RA Dr. iur. Dr. rer. pol.
Fabian Teichmann, LL.M. (London),
MBA (Oxford)*

Abstract

Der Koalitionsvertrag von Union und SPD setzt bei schweren Straftaten auf eine „retrograde biometrische Fernidentifizierung“. Die rechtliche Debatte konzentriert sich dabei häufig auf die Unterscheidung zwischen Echtzeit- und nachträglicher Fernidentifizierung. Der Beitrag zeigt demgegenüber, dass für das Strafverfahren eine andere Trennlinie entscheidend ist: der Datenbestand, gegen den abgeglichen wird. Der Abgleich gegen polizeiliche Referenzdatenbanken wie INPOL unterscheidet sich grundlegend vom Abgleich gegen biometrische Datenbanken, die durch massenhaftes Auslesen von Bildern aus dem Internet erzeugt wurden. Art. 5 Abs. 1 UAbs. 1 lit. e KI-VO sperrt Letzteren nach geltendem Unionsrecht. Zugleich genügen weder die Generalklauseln der StPO noch der gescheiterte Entwurf eines § 98d StPO-E aus dem Sicherheitspaket 2024 oder der Regierungsentwurf vom April 2026 (BT-Drs. 21/6806) den Anforderungen an eine bereichsspezifische Eingriffsnorm. Unter Einbeziehung der hessenDATA-Entscheidung des BVerfG, der §§ 48, 54 BDSG und des Beschlusses des AG Reutlingen zur Pflichtverteidigung bei KI-gestützter Identifizierung arbeitet der Beitrag die Mindestbausteine einer unions- und verfassungskonformen Regelung heraus. Im Ergebnis ist nur ein streng begrenzter Abgleich gegen polizeiinterne Referenzdatenbanken legalisierbar; internetbasierte Gesichtserkennung bleibt dem Staat verwehrt.

The CDU/CSU-SPD coalition agreement envisages “retrospective biometric remote identification” for serious offences. While legal debate has focused on the distinction between real-time and retrospective identification, this article argues that the decisive issue is the database against which biometric data are searched. Searches against police reference databases such as INPOL are fundamentally different, under EU, data protection, and constitutional law, from searches against biometric databases created through the mass harvesting of images from the internet. The latter is precluded by Article 5(1), first

subparagraph, point (e), of the AI Act. Nor do the general provisions of the Code of Criminal Procedure, the failed 2024 draft Section 98d StPO-E, or the Federal Government’s bill of April 2026 (Bundestag printed paper 21/6806) provide an adequate statutory basis. Drawing on the Federal Constitutional Court’s hessenDATA judgment, Sections 48 and 54 BDSG, and the Reutlingen Local Court’s decision on AI-assisted identification, the article sets out the minimum requirements for EU- and constitutionally compliant legislation. It concludes that only narrowly circumscribed searches against police-internal reference databases can be authorised; internet-based facial recognition remains unlawful.

I. Problemstellung und Gang der Untersuchung

Die KI-gestützte Gesichtserkennung gehört zu den Technologien, die den strafprozessualen Gesetzgeber gegenwärtig unter erheblichen Reformdruck setzen.¹ Der Koalitionsvertrag von Union und SPD kündigt an, unter bestimmten, eng definierten Voraussetzungen bei schweren Straftaten eine „retrograde biometrische Fernidentifizierung“ zu ermöglichen.² Das Bundesministerium der Justiz und für Verbraucherschutz (BMJV) hat diesen Regelungsauftrag im März 2026 mit einem Referentenentwurf zur Änderung der Strafprozessordnung aufgegriffen. Die Bundesregierung hat den Entwurf am 29.4.2026 beschlossen und ihn am 1.7.2026 dem Bundestag zugeleitet; nach der ersten Lesung am 8.7.2026 wird er federführend im Ausschuss für Recht und Verbraucherschutz beraten; am 21.9.2026 hat der Innenausschuss eine öffentliche Anhörung zu dem Entwurf und den parallel eingebrachten polizeirechtlichen Entwürfen durchgeführt, in der gerade der biometrische Internetabgleich kontrovers beurteilt wurde (dazu unten VII.). Der Regierungsentwurf sieht einen neuen § 98d StPO-E zum automatisierten biometrischen Abgleich mit im Internet öffentlich zugänglichen Daten sowie – als strafprozessuale Reaktion auf die hessenDATA-Entscheidung des BVerfG – einen § 98e StPO-E

* RA Dr. iur. Dr. rer. pol. Fabian Teichmann, LL.M. (London), MBA (Oxford) ist Rechtsanwalt und Notar in St. Gallen sowie Managing Partner der Teichmann International (Schweiz) AG.

¹ Vgl. Rückert, StV 2025, 350 (356); BR24, Schuldlos in Haft? Das Problem mit KI in der Strafverfolgung, online abrufbar unter: <https://bit.ly/3STTEGQ> (zuletzt abgerufen am 13.4.2026); Uds, Nachwuchskonferenz über KI-Einsatz in der Strafverfolgung und den Schutz der Privatsphäre, online abrufbar unter: <https://bit.ly/46LhuYH> (zuletzt abgerufen am 13.4.2026); zur Kritik an dieser Fokussierung bereits Teichmann, NJOZ 2026, 705 (705 f.); ders., ZfStw 2026, 221 (221 f.).

² CDU CSU, Koalitionsvertrag, online abrufbar unter: <https://bit.ly/3TkWR7m> (zuletzt abgerufen am 25.2.2026), Zeilen 2635-2637, 2852-2853.

zur automatisierten verfahrensübergreifenden Datenanalyse vor.³ Der Regierungsentwurf wird im Folgenden als zentraler Bezugspunkt der Untersuchung behandelt; er belegt, dass die hier vertretene These auch für den neuesten Regelungsanlauf trägt.

Gerade dieser Fall verdeutlicht jedoch, dass „Gesichtserkennung“ strafprozessual keine einheitliche Maßnahme beschreibt. Einerseits setzt das BKA seit Jahren mit „GES“ ein System ein, das Bilder gegen die INPOL-Datenbank abgleicht und damit auf einen begrenzten, bereits polizeilich vorhandenen Datenbestand zugreift.⁴ Andererseits stehen kommerzielle Angebote wie PimEyes oder Clearview AI für ein vollkommen anderes Modell, da sie auf biometrischen Datenbanken beruhen, die durch massenhaftes Auslesen von Gesichtsbildern aus dem Internet aufgebaut wurden.⁵ Zwischen beiden Phänomenen besteht nicht nur ein technischer, sondern vor allem ein normativer Unterschied.

Die zentrale These des vorliegenden Beitrags lautet deshalb, dass die kriminalpolitisch und dogmatisch entscheidende Trennlinie nicht primär zwischen Echtzeit und Nachträglichkeit, sondern zwischen dem Abgleich gegen polizeiinterne Referenzdatenbanken und dem Abgleich gegen internetbasierte biometrische Datenbanken verläuft. Erst auf dieser Grundlage lässt sich beantworten, was der Gesetzgeber regeln darf, was er regeln muss und was er unionsrechtlich gerade nicht legalisieren kann. Nach einer Präzisierung der unterschiedlichen Einsatzformen (II.) werden zunächst die unionsrechtlichen Vorentscheidungen dargestellt (III.), sodann die strafprozessuale Regelungslücke, das Scheitern des § 98d StPO-E im Sicherheitspaket 2024 sowie der Regierungsentwurf vom April 2026 untersucht (IV.), bevor die verfassungs- und beweisrechtlichen Konsequenzen sowie die Eckpunkte einer künftigen Eingriffsnorm entwickelt werden (V. und VI.).

II. Die entscheidende Differenz: Referenzdatenbank statt bloß Echtzeit/Nachträglichkeit

1. Ermittlungsrelevante Einsatzformen

Biometrische Fernidentifizierung kann im Strafverfahren

in unterschiedlichen Konstellationen auftreten. Zu unterscheiden sind jedenfalls vier Grundformen: die Identitätsermittlung durch Abgleich eines unbekannten Gesichts mit einer polizeilichen Referenzdatenbank, die digitale Beobachtung einer bereits individualisierten Person auf Videoaufnahmen, die Echtzeit-Lokalisierung im öffentlichen Raum sowie die retrograde Internetrecherche anhand öffentlich auffindbarer Bilder.⁶ Diese Konstellationen werden in der Debatte häufig unter dem Oberbegriff der „Gesichtserkennung“ zusammengefasst, obwohl sie sich in ihrer Eingriffsintensität erheblich unterscheiden.

Die Identitätsermittlung durch Abgleich gegen INPOL ist die in der Praxis naheliegendste und eingriffsärmere Variante. Sie greift auf einen behördlich vorhandenen Datenbestand zu, der bereits zu polizeilichen Zwecken angelegt worden ist. Demgegenüber verlagert sich die Eingriffsintensität bei der digitalen Beobachtung und mehr noch bei der Echtzeit-Lokalisierung in Richtung einer potenziell lückenlosen Verfolgung von Bewegungen im öffentlichen Raum. Die retrograde Internetrecherche wiederum ist zwar nicht „echtzeitbasiert“, kann aber wegen der ihr zugrundeliegenden Datenbasis besonders weit reichen, weil sie Bilder von Personen erfasst, die in keinerlei Bezug zu einem Strafverfahren stehen.⁷

Die KI-VO differenziert demgegenüber primär zwischen biometrischer Echtzeit-Fernidentifizierung und nachträglicher Fernidentifizierung.⁸ Diese Unterscheidung ist unionsrechtlich wichtig, bildet die strafprozessual entscheidende Eingriffsqualität aber nur unvollkommen ab. Denn nicht jede nachträgliche Fernidentifizierung ist gleich: Der Abgleich eines Beweisfotos gegen INPOL und die Suche mit demselben Foto in einer aus dem Internet ausgescrapten Milliarden-Datenbank sind rechtlich nicht bloß Abstufungen derselben Maßnahme, sondern qualitativ verschiedene Vorgänge.

2. Warum der Datenbestand die Eingriffsqualität prägt

Der Datenbestand entscheidet darüber, ob sich die Maßnahme gegen einen begrenzten, rechtlich vorgeprägten Personenkreis richtet oder faktisch gegen eine unübersehbare Vielzahl Unbeteiligter. Beim Abgleich gegen polizeiliche Referenzdatenbanken greift der Staat auf Daten

³ Gesetzesentwurf der Bundesregierung, Entwurf eines Gesetzes zur Änderung der Strafprozessordnung – digitale Ermittlungsmaßnahmen, BT-Drs. 21/6806 v. 1.7.2026 (Kabinettsbeschluss v. 29.4.2026; zuvor Referentenentwurf des BMJV v. 12.3.2026, online abrufbar unter: <https://bit.ly/4yvN1Kc> [zuletzt abgerufen am 13.4.2026]); Stellungnahme des Bundesrates v. 12.6.2026 und Gegenäußerung der Bundesregierung ebd., S. 26-28; zur ersten Lesung am 8.7.2026 und zur Überweisung an den federführenden Ausschuss für Recht und Verbraucherschutz Deutscher Bundestag, Entwürfe zur Stärkung der digitalen Befugnisse von Ermittlungsbehörden, online abrufbar unter: <https://www.bundestag.de/dokumente/textarchiv/2026/kw28-de-strafprozessordnung-1192534> (zuletzt abgerufen am 13.9.2026); zur öffentlichen Anhörung des Innenausschusses am 21.9.2026 s. die Nachweise in Fn. 57.

⁴ BKA, Gesichtserkennung, online abrufbar unter: <https://bit.ly/4xIOMbP> (zuletzt abgerufen am 13.4.2026); Rückert, StV 2025, 350 (356).

⁵ Martini/Kemper, CR 2023, 341 ff.; Martini, NVwZ - Extra 2022, 1 (2 ff.).

⁶ Coombe/Roth-Isigkeit, ZfDR 2024, 391 (395 ff.).

⁷ Medienservice Sachsen, Erfolgsmodell „PerIS“ wird erweitert – Polizei nimmt neue Kameras in Zittau in Betrieb, online abrufbar unter: <https://bit.ly/3SEz7pU> (zuletzt abgerufen am 13.4.2026); Die Zeit, Polizei installiert Kameras zur Kriminalitätsbekämpfung, online abrufbar unter: <https://bit.ly/3V0ff12> (zuletzt abgerufen am 13.4.2026); Deutscher Bundestag, Fachbereiche EU 6 und WD 5, Biometrischer Abgleich mit Bildern aus dem Internet, Das technische Gutachten im Auftrag von AlgorithmWatch, online abrufbar unter: <https://bit.ly/3Vlw72n> (zuletzt abgerufen am 13.4.2026), S. 6-10.

⁸ Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13.6.2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz, Art. 3 Nr. 41-44 – nachfolgend Verordnung (EU) 2024/1689 genannt; Hilgendorf/Härtlein, in: HK-KI-VO, 2025, Art. 3 Rn. 43-46; Kirschke-Biller/Füllsack, in: BeckOK-KI-Recht, 5. Ed. (Stand: 1.11.2025), KI-VO Art. 3 Rn. 485-498, 499-506.1, 507-513, 514-526.

zurück, die jedenfalls nicht erst für die konkrete Maßnahme aus dem offenen Netz zusammengesucht werden mussten. Der Abgleich gegen im Internet gewonnene biometrische Datenbanken setzt demgegenüber gerade voraus, dass Gesichter ungezielt, massenhaft und ohne konkreten Verfahrensbezug erfasst und in mathematisch vergleichbare Merkmalsvektoren überführt werden.⁹ Die Eingriffsintensität steigt deshalb nicht nur wegen der Menge der Daten, sondern auch wegen der Breite des betroffenen Personenkreises.

Hinzu kommt, dass die Systeme keineswegs fehlerfrei arbeiten. Zwar haben sich die Erkennungsraten in den vergangenen Jahren deutlich verbessert; gleichzeitig zeigen Studien des NIST und der EU-Grundrechteagentur, dass Fehlerquoten nach Hautfarbe, Geschlecht und Alter variieren können.¹⁰ Die Wahl der Referenzdatenbank ist damit nicht nur eine Frage des Umfangs, sondern auch der Verteilungswirkungen des Eingriffs. Ein gesetzlicher Zugriff auf besonders breite Datenbestände vergrößert zwangsläufig das Risiko systematischer Fehlzuordnungen und diskriminierender Effekte.

Gerade deshalb verfehlt es die Diskussion, wenn sie die Kategorie der „nachträglichen Fernidentifizierung“ als einheitlichen Legalisierungsraum behandelt. Aus strafprozessualer Sicht ist nicht entscheidend, dass die Identifizierung zeitlich nachgelagert erfolgt, sondern auf welchen Datenkörper der Staat zugreift und welche Personen dadurch in die Maßnahme einbezogen werden. Die nachfolgende unionsrechtliche Analyse bestätigt genau diese Sichtweise.

III. Unionsrechtliche Vorprägung

1. Art. 5 Abs. 1 UAbs. 1 lit. e KI-VO als Sperre für den Internetabgleich

Die KI-VO beansprucht grundsätzlich auch für das nationale Polizei- und Strafverfahrensrecht Geltung; die Ausnahme für die nationale Sicherheit greift für die Strafverfolgung gerade nicht ein.¹¹ Für die hier interessierende

Frage ist zunächst Art. 5 Abs. 1 UAbs. 1 lit. e KI-VO zentral. Danach ist die Erstellung oder Erweiterung von Datenbanken zur Gesichtserkennung durch das ungezielte Auslesen von Gesichtsbildern aus dem Internet oder aus Überwachungsaufnahmen verboten.¹² Das Verbot ist ausnahmslos formuliert und kennt namentlich keine Privilegierung staatlicher Stellen.

Damit ist der unionsrechtliche Befund härter, als es manche kriminalpolitische Debatte suggeriert. Wer einen biometrischen Abgleich mit Bildern aus dem offenen Internet ermöglichen will, benötigt hierfür technisch eine Datenbank, in der die im Netz aufgefundenen Gesichter bereits extrahiert und in biometrisch vergleichbare Datensätze übersetzt worden sind. Genau dies hat das im Auftrag von AlgorithmWatch erstellte und vom Deutschen Bundestag ausgewertete Gutachten von *Lewandowski* herausgearbeitet.¹³ Das unionsrechtliche Problem liegt folglich nicht erst in der konkreten Suchanfrage der Strafverfolgungsbehörde, sondern vorgelagert im Aufbau des Datenbestands selbst.

Die Konsequenz ist eindeutig: Solange der Internetabgleich technisch auf solchen Datenbanken beruht, steht Art. 5 Abs. 1 UAbs. 1 lit. e KI-VO einer strafprozessualen Legalisierung entgegen. Der Gesetzgeber kann dieses Hindernis nicht dadurch neutralisieren, dass er die Maßnahme im nationalen Recht als „retrograd“ etikettiert. Die Leitlinien der Kommission und die deutsche Aufsichtspraxis bestätigen, dass verbotene Praktiken nicht durch nationale Zweckbestimmungen umdefiniert werden können.¹⁴ Der Koalitionsvertrag markiert damit zwar ein kriminalpolitisches Interesse, löst aber das unionsrechtliche Dilemma nicht auf.

2. Echtzeit-Fernidentifizierung, öffentlicher Raum und Hochrisikoanforderungen

Neben lit. e ist Art. 5 Abs. 1 UAbs. 1 lit. h KI-VO zu beachten. Die biometrische Echtzeit-Fernidentifizierung in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken ist grundsätzlich verboten und nur in eng begrenzten

⁹ Verordnung (EU) 2024/1689, Art. 5 Abs. 1 lit. e, ErwG 43; *Wendehorst*, in: Martini, KI-VO, 2. Aufl. (2026), Art. 5 Rn. 139-141; *Raue*, in: BeckOK-KI-Recht, KI-VO Art. 5 Rn. 82-88; *Hilgendorf/Härtlein*, in: HK-KI-VO, Art. 5 Rn. 45-48; *Reuter*, Datenschutz-Verfahren gegen PimEyes und Clearview, online abrufbar unter: <https://bit.ly/3V3Nchb> (zuletzt abgerufen am 13.4.2026); Handelsblatt, Clearview legt offenbar Datenbank mit Milliarden Fotos zur Gesichtserkennung an, online abrufbar unter: <https://bit.ly/4dtxNNw> (zuletzt abgerufen am 13.4.2026); Spiegel, Clearview AI muss 30,5 Millionen Euro Strafe in den Niederlanden zahlen, online abrufbar unter: <https://bit.ly/3Tkyyle> (zuletzt abgerufen am 13.4.2026); *Teichmann*, ZfIStw 2026, 221 (224); *ders.*, NJOZ 2026, 705 (707).

¹⁰ NIST, Face Recognition Vendor Test (FRVT) – Demographic Effects, online abrufbar unter: <https://bit.ly/4ytpfW> (zuletzt abgerufen am 13.4.2026), S. 28 ff.; *Buolamwini/Gebbru*, PMLR 2018, 1 ff.; FRA, Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement, online abrufbar unter: <https://bit.ly/3SU4PiY> (zuletzt abgerufen am 13.4.2026), Ziff. 3.3.

¹¹ Verordnung (EU) 2024/1689, Art. 2 Abs. 3; *Voigt*, in: BeckOK-KI-Recht, 5. Ed. (Stand: 1.11.2025), KI-VO Art. 2 Rn. 36-39; *Hilgendorf/Härtlein*, in: HK-KI-VO, 2025, Art. 2 Rn. 11.

¹² Verordnung (EU) 2024/1689, Art. 5 Abs. 1 lit. e; *Raue*, in: BeckOK-KI-Recht, KI-VO Art. 5 Rn. 82-88; *Hilgendorf/Härtlein*, in: HK-KI-VO, Art. 5 Rn. 45-48; *Wendehorst*, in: Martini, KI-VO, 2. Aufl. (2026), Art. 5 Rn. 139-141.

¹³ *Lewandowski*, Braucht die Polizei eine Datenbank zum biometrischen Abgleich?, online abrufbar unter: <https://algorithm-watch.org/de/wp-content/uploads/2025/10/2025-AW-Gutachten-V9.pdf> (zuletzt abgerufen am 13.9.2026); Deutscher Bundestag, Biometrischer Abgleich mit Bildern aus dem Internet, online abrufbar unter: <https://bit.ly/4xNC1I8> (zuletzt abgerufen am 13.4.2026), S. 6-10.

¹⁴ Bundesnetzagentur, Art. 5 der KI-Verordnung (Verbotene Praktiken), online abrufbar unter: <https://bit.ly/3UMgAbK> (zuletzt abgerufen am 13.4.2026); Europäische Kommission, Die Kommission veröffentlicht die Leitlinien zu verbotenen Praktiken der künstlichen Intelligenz (KI) im Sinne des KI-Gesetzes, online abrufbar unter: <https://bit.ly/4ysnNML> (zuletzt abgerufen am 13.4.2026); Amnesty, Deutschland: Biometrische Überwachungspläne der Bundesregierung sind zum Scheitern verurteilt, online abrufbar unter: <https://bit.ly/4xQObjA> (zuletzt abgerufen am 13.4.2026).

Ausnahmefällen zulässig.¹⁵ Zwar ist dogmatisch nicht in jeder Konstellation eindeutig, wie weit der Begriff des „öffentlich zugänglichen Ortes“ reicht; insbesondere internetbasierte Suchen spielen sich nicht notwendig an einem physischen Ort im Sinne des Art. 3 Nr. 44 KI-VO ab.¹⁶ Für den Internetabgleich bedarf diese Abgrenzung aber letztlich keiner Vertiefung, weil schon das Verbot des Datenbankaufbaus nach lit. e die Maßnahme blockiert.

Anders stellt sich die Lage bei zulässigen, nachträglichen Abgleichen gegen bestehende Referenzdatenbanken dar. Solche Systeme sind als Hochrisiko-KI-Systeme einzuordnen und unterliegen deshalb den umfangreichen Anforderungen der KI-VO: Risikomanagement, Qualität der Trainings- und Testdaten, technische Dokumentation, Protokollierung, Transparenz, menschliche Aufsicht sowie die besonderen Genehmigungsvorgaben des Art. 26 Abs. 10 KI-VO.¹⁷ Die KI-VO eröffnet also keinen rechtsfreien Raum für „bloß nachträgliche“ Gesichtserkennung, sondern koppelt auch die grundsätzlich zulässigen Varianten an einen dichten Schutzmechanismus.

Die unionsrechtliche Vorprägung läuft damit auf eine doppelte Aussage hinaus. Erstens ist der internetbasierte Abgleich mit ausgescrapten biometrischen Datenbanken gesperrt. Zweitens ist der Abgleich gegen sonstige Referenzdatenbestände nur dann denkbar, wenn der nationale Gesetzgeber eine spezifische Eingriffsnorm schafft, die die unionsrechtlichen Schutzanforderungen nicht unterschreitet.

3. *JI-Richtlinie und BDSG*

Neben der KI-VO bildet die Richtlinie (EU) 2016/680 den zweiten unionsrechtlichen Bezugsrahmen. Sie ist für die Tätigkeit der Strafverfolgungsbehörden maßgeblich und in den §§ 45 ff. BDSG umgesetzt worden.¹⁸ Das ist deshalb bedeutsam, weil die unionsrechtliche Bewertung biometrischer Fernidentifizierung nicht auf die KI-VO reduziert werden darf. Auch ein nach der KI-VO nicht verbotenes System ist nur dann zulässig, wenn die daten-

schutzrechtlichen Anforderungen des JI-Regimes eingehalten werden.

Für biometrische Daten ist insbesondere § 48 BDSG einschlägig. Die Vorschrift verlangt, dass die Verarbeitung besonderer Kategorien personenbezogener Daten – und dazu gehören biometrische Daten – für die jeweilige Maßnahme unbedingt erforderlich sein muss und von geeigneten Garantien für die Rechte und Freiheiten der betroffenen Personen begleitet wird.¹⁹ Eine künftige Eingriffsnorm kann sich deshalb nicht darauf beschränken, den Einsatz abstrakt zu erlauben. Sie muss vielmehr die besonderen technisch-organisatorischen Sicherungen zumindest im Kern normativ absichern.

Ebenso wichtig ist § 54 BDSG. Nachteilige Entscheidungen dürfen nicht ausschließlich auf einer automatisierten Verarbeitung beruhen.²⁰ Für das Strafverfahren bedeutet das, dass ein softwaregestützter Treffer weder den Tatverdacht „automatisch“ begründen noch ohne echte inhaltliche Prüfung weitere belastende Maßnahmen tragen darf. Menschliche Verifikation ist deshalb kein bloßes Qualitätsversprechen, sondern unionsrechtlich geboten.

IV. Die nationale Regelungslücke

1. *Unzulänglichkeit der vorhandenen StPO-Normen*

Die geltende Strafprozessordnung enthält keine bereichsspezifische Eingriffsnorm für den Einsatz biometrischer Fernidentifizierung. Die Generalklauseln der §§ 161, 163 StPO scheiden als Rechtsgrundlage aus. Nach der Rechtsprechung des *BVerfG* und der aus Art. 80 GG abgeleiteten Wesentlichkeits- und Bestimmtheitsdogmatik bedürfen eingriffsintensive Ermittlungsmaßnahmen einer hinreichend bestimmten gesetzlichen Grundlage; Annexkompetenzen und generalisierte Ermittlungsbefugnisse genügen dafür nicht.²¹

Ebenso wenig trägt der Versuch, die Maßnahme aus einer Kombination einzelner Vorschriften wie §§ 98a, 98c, 100h oder 163f StPO herzuleiten. Eine solche Normku-

¹⁵ Verordnung (EU) 2024/1689, Art. 5 Abs. 1 lit. h, ErwG 17, 32; *Hilgendorf/Härtlein*, in: HK-KI-VO, Art. 5 Rn. 67; *Raue*, in: BeckOK-KI-Recht, KI-VO Art. 5 Rn. 111-113; *Wendehorst*, in: Martini, KI-VO, Art. 5 Rn. 206-207.

¹⁶ Verordnung (EU) 2024/1689, Art. 3 Nr. 44; *Hilgendorf/Härtlein*, in: HK-KI-VO, Art. 3 Rn. 46; *Wendehorst*, in: Martini, KI-VO, Art. 3 Rn. 335-340.

¹⁷ Verordnung (EU) 2024/1689, Art. 6 Abs. 2 i.V.m. Anhang III Nr. 1 lit. a, ErwGr. 17, 52; *Hilgendorf/Härtlein*, in: HK-KI-VO, Art. 6 Rn. 10-11, Art. 26 Rn. 14-15; *Klawonn*, in: BeckOK-KI-Recht, KI-VO Art. 6 Rn. 16-18; *Denga*, in: BeckOK-KI-Recht, KI-VO Art. 26 Rn. 77; *Wendehorst*, in: Martini, KI-VO, Art. 9 Rn. 15-19, Art. 10 Rn. 10-14, Art. 11 Rn. 10, Art. 12 Rn. 8-11, Art. 13 Rn. 1-2, Art. 14 Rn. 2-4, Art. 26 Rn. 68-70.

¹⁸ Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr; *Wolff/von Ungern-Sternberg*, in: BeckOK-DatenschutzR, 54. Ed. (Stand: 1.11.2025), BDSG § 45 Rn. 4; *Braun*, in: Gola/Heckmann, BDSG, 3. Aufl. (2022), § 45 Rn. 1-4; *Frenzel*, in: Paal/Pauly, BDSG, 4. Aufl. (2026), § 45 Rn. 1-5.

¹⁹ *Kampert*, in: Sydow/Marsch DS-GVO/BDSG, 3. Aufl. (2022), BDSG § 48 Rn. 9, 13-16; *Schwichtenberg*, in: Kühling/Buchner, 4. Aufl. (2024), BDSG § 48 Rn. 2-6; *Albers/Schimke*, in: BeckOK-DatenschutzR, BDSG § 48 Rn. 16-28, 33-41; *Frenzel*, in: Paal/Pauly, DS-GVO/BDSG, BDSG § 48 Rn. 3-9.

²⁰ Richtlinie (EU) 2016/680, Art. 11; *Mundil*, in: BeckOK-DatenschutzR, BDSG § 54 Rn. 1-3b; *Frenzel*, in: Paal/Pauly, DS-GVO BDSG, BDSG § 54 Rn. 1-9; *Schwichtenberg*, in: Kühling/Buchner, DS-GVO/BDSG, BDSG § 54 Rn. 4-5; *Richter*, in: Simitis/Hor-nung/Spiecker gen. Döhmman, Datenschutzrecht, 2. Aufl. (2025), § 54 Rn. 3-7.

²¹ *BVerfG*, Beschl. v. 18.12.2018 – 1 BvR 142/15, Rn. 21 ff.; *BVerfG*, Beschl. v. 30.12.2012 – 1 BvR 502/09, Rn. 4; *Martini*, NVwZ-Extra 1-2/2022, 10 (11); *Remmert*, in: Dürig/Herzog/Scholz, GG, 108. EL (Stand: 08/2025), Art. 80 Rn. 69-73; *Uhle*, in: BeckOK-GG, 64. Ed. (Stand: 15.9.2025), Art. 80 Rn. 17-31.

mulation zerlegt eine einheitliche biometrische Fernidentifizierung künstlich in Teilakte, obwohl gerade die Verknüpfung von automatisierter Bildgewinnung, biometrischer Extraktion und Datenbankabgleich die neue Eingriffsqualität erzeugt. Die Datenschutzaufsicht hat deshalb zutreffend darauf hingewiesen, dass die bestehenden Vorschriften den grundrechtlichen Anforderungen an die Gesichtserkennung nicht gerecht werden.²²

Die strafprozessuale Ausgangslage ist damit klar: Es fehlt an einer eigenständigen, auf die biometrische Fernidentifizierung zugeschnittenen Ermächtigung. Solange eine solche Norm nicht existiert, bleibt der Einsatz nicht deshalb zulässig, weil er kriminalistisch attraktiv erscheint oder technisch ohne großen Aufwand durchgeführt werden könnte.

2. Die Defizite des § 98d StPO-E im Sicherheitspaket 2024

Der im Rahmen des sogenannten Sicherheitspakets vorgelegte Entwurf eines § 98d StPO-E zielte auf den nachträglichen Abgleich von Bild- und Stimmmerkmalen mit öffentlich zugänglichen Daten aus dem Internet.²³ Der Entwurf enthielt durchaus Elemente, die bei einer künftigen Regelung in Betracht kommen können, etwa den Richtervorbehalt und die Beschränkung auf schwere Straftaten. Sein Kernproblem lag aber darin, dass er die unionsrechtlich entscheidende Vorfrage offenließ: Mit welcher Datenbank soll der biometrische Abgleich eigentlich durchgeführt werden?

Gerade diese Leerstelle war nicht technischer Natur, sondern rechtlich fatal. Wenn der Internetabgleich, wie gezeigt, zwingend auf Datenbanken beruht, deren Erstellung Art. 5 Abs. 1 UAbs. 1 lit. e KI-VO verbietet, kann eine nationale Norm die Maßnahme nicht legalisieren, sondern allenfalls in Widerspruch zum Unionsrecht setzen.²⁴ Hinzu kam, dass der Entwurf keine hinreichend konkreten Schutzmaßnahmen für biometrische Daten, keine klare Antwort auf systemimmanente Diskriminierungsrisiken und keine tragfähige Regelung zur menschlichen Kontrolle enthielt.²⁵

Der Entwurf scheiterte im Bundesrat zudem nicht etwa an einem datenschutzrechtlichen Übermaß, sondern aus parteipolitischen Gründen, namentlich wegen des Streits um

weitere sicherheitspolitische Begleitmaßnahmen.²⁶ Gerade das zeigt, dass die materiellen Defizite des § 98d StPO-E durch sein politisches Scheitern nicht „erledigt“ sind. Sie werden vielmehr jede künftige Neuregelung erneut einholen.

3. Der Regierungsentwurf vom April 2026 zwischen punktuelltem Fortschritt und unionsrechtlicher Sperre

Der von der Bundesregierung am 29.4.2026 beschlossene Entwurf unternimmt einen neuen Anlauf zur Schaffung einer bereichsspezifischen Rechtsgrundlage. § 98d StPO-E n.F. soll den automatisierten biometrischen Abgleich zwischen Daten aus einem Strafverfahren und „im Internet öffentlich zugänglichen biometrischen Daten“ bei Straftaten von „auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Abs. 2 bezeichnete Straftat“, ermöglichen.²⁷ § 98e StPO-E n.F. ergänzt hierzu eine Befugnis zur automatisierten verfahrensübergreifenden Datenanalyse, die als strafprozessuale Parallelnorm zu den nach der hessenDATA-Entscheidung erneuerten landesrechtlichen Ermächtigungsgrundlagen konzipiert ist.²⁸

Der Entwurf erkennt die unionsrechtliche Vorfrage zumindest teilweise, denn die Begründung zu Abs. 1 und 3 schließt die Einrichtung einer dauerhaften Datenbank, die sämtliche aus dem Internet erhobenen Lichtbilder und die zugehörigen Templates enthält, ausdrücklich aus und beschränkt die temporäre Speicherung auf den Zweck des konkreten Ausgangsverfahrens; auch aus den erhobenen Daten gewonnene Templates sind nach Abschluss des Abgleichs zu löschen.²⁹ Diese Eingrenzung markiert gegenüber dem Sicherheitspaket-Entwurf 2024 einen Schutzfortschritt auf der Verwendungs- und Speicherebene.

Sie löst das unionsrechtliche Grundproblem jedoch nicht. Art. 5 Abs. 1 UAbs. 1 lit. e KI-VO knüpft das Verbot an die „Erstellung oder Erweiterung“ einer Erkennungsdatenbank durch ungezieltes Auslesen, ohne nach Dauer, Zweck oder anschließender Löschung zu differenzieren. Auch eine ad hoc und ausschließlich für ein konkretes Strafverfahren aufgebaute, anschließend gelöschte biometrische Suchdatenbank erfüllt den Verbotstatbestand; die Löschpflicht des § 98d Abs. 3 StPO-E n.F. setzt zeitlich nach dem unionsrechtlichen Verbotszeitpunkt an und kann ihn folglich nicht heilen.³⁰ Der Schutzzweck der Norm zielt nach den Erwägungsgründen 17 und 32 auf die

²² DSK, Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 20. September 2024, online abrufbar unter: <https://bit.ly/3SPISv3> (zuletzt abgerufen am 13.4.2026); *Koranyi/Singelstein*, NJW 2011, 124 (128); *Singelstein*, NSiZ 2012, 593 ff.

²³ BT-Drs. 20/12806, S. 14; *Lewandowski* (Fn. 13).

²⁴ *Lewandowski* (Fn. 13); *Deutscher Bundestag* (Fn. 13), S. 6-10.

²⁵ *Kampert*, in: *Sydow/Marsch DS-GVO/BDSG, BDSG* § 48 Rn. 9, 13-16; *Schwichtenberg*, in: *Kühling/Buchner, BDSG* § 48 Rn. 2-6; *Albers/Schimke*, in: *BeckOK-DatenschutzR, BDSG* § 48 Rn. 16-28, 33-41; *Frenzel*, in: *Paal/Pauly, DS-GVO/BDSG, BDSG* § 48 Rn. 3-9.

²⁶ Beck-aktuell, Verfassungsrechtliche Bedenken: Sicherheitspaket lässt auf sich warten, online abrufbar unter: <https://bit.ly/4ysIEk0> (zuletzt abgerufen am 13.4.2026); Spiegel, Bundesrat lässt Teile des Sicherheitspakets durchfallen, online abrufbar unter: <https://bit.ly/4ynPpT1> (zuletzt abgerufen am 13.4.2026); Handelsblatt, Ampel-Sicherheitspaket fällt im Bundesrat teilweise durch, online abrufbar unter: <https://bit.ly/46bGJ6r> (zuletzt abgerufen am 13.4.2026).

²⁷ BT-Drs. 21/6806, S. 7, 15 ff.; zum Regierungsentwurf bereits *Teichmann*, ZfStw 2026, 221 (228).

²⁸ BT-Drs. 21/6806, S. 8 f., 18 ff.; *BVerfG*, Urt. v. 16.2.2023 – 1 BvR 1547/19 u.a.

²⁹ BT-Drs. 21/6806, S. 16 f.

³⁰ *Lewandowski* (Fn. 13); *Deutscher Bundestag* (Fn. 13), S. 6-10; *Hilgendorf/Härtlein*, in: *HK-KI-VO*, Art. 5 Rn. 45-48; *Raue*, in: *BeckOK-KI-Recht, KI-VO* Art. 5 Rn. 82-88; *Wendehorst*, in: *Martini, KI-VO*, Art. 5 Rn. 139-141; *Verordnung (EU) 2024/1689*, ErwGr. 17, 32.

Verhinderung biometrischer Erfassungsinfrastruktur als solche und nicht erst auf deren Verstetigung.

Hinzu kommt ein in der Begründung selbst angelegtes Strukturproblem. Soweit die deutschen Strafverfolgungsbehörden den Abgleich technisch nicht selbst durchführen können, sieht die Begründung den Weg über die justizielle Rechtshilfe nach den §§ 77d ff. IRG vor und verweist auf eine – inzwischen ebenfalls als Regierungsentwurf vorliegende – Begleitnovelle des BKAG, die dem Bundeskriminalamt in seiner Zentralstellenfunktion ermöglichen soll, im Falle von Straftaten zum Schutz der nationalen Sicherheit an Anbieter in einem Drittstaat heranzutreten – nach dem Wortlaut der Begründung „auch private Anbieter“.³¹ Damit etabliert der Entwurf einen Pfad, auf dem die deutsche Strafverfolgung mittelbar genau jene biometrischen Scraping-Datenbanken nutzbar machen würde, deren Erstellung Art. 5 Abs. 1 UAbs. 1 lit. e KI-VO untersagt. Da der Verbotstatbestand neben dem Inverkehrbringen und der Inbetriebnahme ausdrücklich auch die „Verwendung“ erfasst, schließt er diese mittelbare Inanspruchnahme erkennbar mit ein.³² Die innerstaatliche Löschpflicht des § 98d Abs. 3 StPO-E n.F. kann diesen Strukturkonflikt nicht auflösen, weil sie das Verbot des Datenbankaufbaus auf Anbieterseite gerade unberührt lässt. Die Beschränkung der BKAG-Begleitnovelle auf Fälle der nationalen Sicherheit mildert das Problem im Anwendungsbereich, beseitigt es aber nicht.

Die Begründung versucht, der unionsrechtlichen Hürde zusätzlich durch eine engere Auslegung des Verbotstatbestands zu entgehen: Das Verbot greife nicht, „sofern für das Auslesen der Daten keine KI-Systeme eingesetzt werden“.³³ Diese Argumentation, die sich auf Rn. 234 der Kommissionsleitlinien stützt, überzeugt nicht. Maßgeblich ist nicht die Technik des Auslesungsvorgangs, sondern dessen funktionaler Zweck, also die Erstellung oder Erweiterung einer Erkennungsdatenbank. Andernfalls würde das Verbot bei rein prozeduralem, nicht KI-gestütztem Scraping leerlaufen, obwohl das Resultat – eine biometrisch durchsuchbare Datenbank ohne Rechtsgrundlage in der Person der Betroffenen – identisch wäre.³⁴

Auf verfahrensrechtlicher Ebene fehlt dem Entwurf zudem ein Richtervorbehalt. § 98d Abs. 4 StPO-E n.F. weist die Anordnungskompetenz primär der Staatsanwaltschaft zu; bei Gefahr im Verzug dürfen sogar Ermittlungspersonen nach § 152 GVG anordnen, wobei die staatsanwaltschaftliche Bestätigung binnen 48 Stunden zu erfolgen hat.³⁵ Der Entwurf bleibt damit eine systematische Stufe

unter dem für vergleichbar eingriffsintensive Ermittlungsmaßnahmen üblichen Anordnungsregime. Für die Telekommunikationsüberwachung als ebenfalls tiefgreifenden Eingriff in das informationelle Selbstbestimmungsrecht ordnet § 100e Abs. 1 StPO einen grundsätzlichen Richtervorbehalt an, an dessen Stelle nur in Eilfällen die Staatsanwaltschaft tritt. Eine entsprechende Stufung – Richter im Regelfall, Staatsanwaltschaft in Eilfällen – wäre auch für die biometrische Fernidentifizierung sachlich geboten und vom *BVerfG* für vergleichbar tiefgreifende Eingriffe in das informationelle Selbstbestimmungsrecht im Grundsatz verlangt.³⁶ Die Begründung leitet das abgesenkte Schutzniveau aus Art. 26 Abs. 10 KI-VO ab, der lediglich eine Entscheidung einer „Justiz- oder Verwaltungsbehörde“ verlangt.³⁷ Dieser Verweis ist rechtstechnisch zutreffend, aber verfassungsrechtlich nicht tragfähig. Art. 26 Abs. 10 KI-VO markiert eine unionsrechtliche Mindestschwelle und enthebt den nationalen Gesetzgeber nicht der Pflicht, das verfassungsrechtlich gebotene Schutzniveau zu wahren.³⁸

Schließlich wird der Entwurf den aus § 54 BDSG und Art. 14 Abs. 5 KI-VO folgenden Anforderungen an die menschliche Verifikation nur eingeschränkt gerecht. Während § 98e Abs. 4 S. 4 StPO-E n.F. für die verfahrensübergreifende Datenanalyse ausdrücklich klarstellt, dass eine ausschließlich automatisierte Entscheidungsfindung mit nachteiligen Rechtsfolgen unzulässig ist, fehlt eine entsprechende Klarstellung für den biometrischen Abgleich nach § 98d StPO-E n.F. im Entwurfstext selbst. Die Begründung verweist insoweit lediglich auf die unmittelbare Geltung des Art. 14 Abs. 5 KI-VO und beschreibt in den Erläuterungen zu Abs. 2 eine Prüfung der morphologischen Übereinstimmung durch die Ermittlungsbeamten, ohne dies im Normtext zu verankern.³⁹ Für eine bereichsspezifische Eingriffsnorm, die den vom *BVerfG* geforderten normativen Garantien genügen soll, ist dieser externe Verweis zu dünn.

V. Verfassungs- und beweisrechtliche Konsequenzen

1. hessenDATA als Leitentscheidung

Verfassungsrechtlich ist die Entscheidung des *BVerfG* zur automatisierten Datenanalyse in Hessen und Hamburg der zentrale Bezugspunkt. Das Gericht hat hervorgehoben, dass automatisierte Datenanalyse nicht bloß vorhandene Informationen zusammenführt, sondern qualitativ neues Wissen erzeugt und gerade deshalb ein eigenständiges Eingriffsgewicht besitzt.⁴⁰ Diese Überlegung lässt sich

³¹ BT-Drs. 21/6806, S. 17; die dort angekündigte Begleitnovelle liegt inzwischen als Gesetzentwurf der Bundesregierung vor: BT-Drs. 21/6132 v. 26.5.2026 (§ 9a BKAG-E), flankiert von BT-Drs. 21/6131 v. 26.5.2026; beide wurden am 8.7.2026 gemeinsam mit BT-Drs. 21/6806 in erster Lesung beraten.

³² Raue, in: BeckOK-KI-Recht, KI-VO Art. 5 Rn. 82-88; Wendehorst, in: Martini, KI-VO, Art. 5 Rn. 139-141; Hilgendorf/Härtlein, in: HK-KI-VO, Art. 5 Rn. 45-48.

³³ BT-Drs. 21/6806, S. 14 f.

³⁴ Vgl. Hilgendorf/Härtlein, in: HK-KI-VO, Art. 5 Rn. 45-48; Raue, in: BeckOK-KI-Recht, KI-VO Art. 5 Rn. 82-88; Verordnung (EU) 2024/1689, ErwGr. 17, 32; Europäische Kommission (Fn. 14), Rn. 234.

³⁵ BT-Drs. 21/6806, S. 8.

³⁶ Meyer-Goßner/Schmitt, StPO, 67. Aufl. (2024), § 100e Rn. 1 ff.; Bruns, in: KK-StPO, 9. Aufl. (2023), StPO § 100e Rn. 1-4; *BVerfG*, Urt. v. 16.2.2023 – 1 BvR 1547/19 u.a., Rn. 91 ff., 150 f.

³⁷ BT-Drs. 21/6806, S. 17 f.

³⁸ Remmert, in: Dürig/Herzog/Scholz, GG, Art. 80 Rn. 69-73; Uhle, in: BeckOK-GG, Art. 80 Rn. 17-31.

³⁹ BT-Drs. 21/6806, S. 14, 16 f.

⁴⁰ *BVerfG*, Urt. v. 16.2.2023 – 1 BvR 1547/19, 1 BvR 2634/20, Rn. 50, 62, 71; GFF, GFF erhebt Verfassungsbeschwerde gegen Gesetzesnovelle: Hessen setzt verfassungswidrige BIG-DATA-Analyse fort, online abrufbar unter: <https://bit.ly/4r59T0r> (zuletzt abgerufen am 13.4.2026); Rudl, Erneute Verfassungsbeschwerde gegen polizeiliche Big-Data-Analysen, online abrufbar unter: <https://bit.ly/4gHreJs> (zuletzt abgerufen am 13.4.2026).

auf die biometrische Gesichtserkennung ohne weiteres übertragen, und zwar eher in verschärfter als in abgeschwächter Form.

Das liegt zum einen an der Qualität der betroffenen Daten. Biometrische Merkmale sind nicht austauschbar, sondern an die Person dauerhaft gebunden. Zum anderen können großskalige Gesichtserkennungssysteme potentiell eine Vielzahl Unbeteiligter erfassen und durch Fehlerrisiken ungleich belasten. Je breiter der einbezogene Datenbestand, desto näher rückt die Maßnahme an eine allgemeine Infrastruktur biometrischer Katalogisierung heran.⁴¹ Das *BVerfG* verlangt deshalb eine bereichsspezifische Eingriffsnorm, die Eingriffsschwelle, Zweckbindung, Verfahren und Sicherungen klar bestimmt.⁴²

Für die Gesichtserkennung lassen sich daraus mindestens acht Anforderungen ableiten: eine eigenständige Rechtsgrundlage, eine qualifizierte Eingriffsschwelle, strikte Subsidiarität, richterliche Anordnung, echte menschliche Kontrolle, Dokumentations- und Transparenzpflichten, gesetzlich abgesicherter Schutz vor diskriminierenden Systemeffekten und eine unionsrechtskonforme Datengrundlage. Diese Anforderungen sind nicht additiver „Luxus“, sondern die Konsequenz daraus, dass biometrische Fernidentifizierung nicht bloße Effizienzsteigerung klassischer Ermittlungsarbeit ist, sondern eine qualitativ andere Form automatisierter Personenbestimmung.

Der § 98e StPO-E n.F. des Regierungsentwurfs stellt den unmittelbaren Versuch dar, die vom *BVerfG* aufgestellten Anforderungen strafprozessual umzusetzen.⁴³ Die Norm beschränkt die automatisierte Datenanalyse auf rechtmäßig gespeicherte Daten aus polizeilichen Informationssystemen, schließt Daten aus Online-Durchsuchung und Wohnraumüberwachung gemäß §§ 100b, 100c StPO ausdrücklich aus (§ 98e Abs. 2 S. 3 StPO-E n.F.) und verbietet eine direkte Anbindung der Analyseplattform an nicht-polizeiliche Register sowie an Internetdienste (§ 98e Abs. 3 S. 1 StPO-E n.F.). § 98e Abs. 4 S. 4 StPO-E n.F. untersagt überdies eine ausschließlich automatisierte Entscheidungsfindung mit nachteiligen Rechtsfolgen und verpflichtet in Satz 5 zu einer technisch-organisatorischen Vermeidung diskriminierender Algorithmen. Diese Grenzziehungen sind jedenfalls im Ansatz vom *BVerfG* vorgezeichnet.⁴⁴

Für die hier in den Blick genommene biometrische Fernidentifizierung ergibt sich allerdings eine bemerkenswerte Ungleichgewichtigkeit: Während § 98e StPO-E n.F.

für die verfahrensübergreifende Analyse enge methodische und datenseitige Grenzen aufrichtet, verzichtet § 98d StPO-E n.F. für den biometrischen Internetabgleich auf eine vergleichbare Datenbankbeschränkung – und erlaubt in den Begründungserläuterungen zu Abs. 3 sogar den mittelbaren Zugriff auf private Anbieter in Drittstaaten. Obwohl in beiden Fällen hochsensible personenbezogene Daten betroffen sind und obwohl biometrische Daten einer höheren Schutzintensität unterliegen als Vorgangs- und Falldaten der Polizei, fällt das Schutzniveau beim biometrischen Abgleich hinter das für die Datenanalyse vorgesehene zurück. Diese Regulationsasymmetrie ist nicht zu rechtfertigen; sie bestätigt die hier vertretene These, dass die entscheidende Trennlinie im Referenzdatenbestand liegt, nicht im zeitlichen Bezug der Maßnahme. Bezeichnenderweise hat der Bundesrat in seiner Stellungnahme vom 12.6.2026 allein § 98e StPO-E n.F. beanstandet – nicht als zu weit, sondern als zu eng, weil die Norm keine eigenständige Zusammenführungsbefugnis enthält und staatsanwaltschaftliche Daten ausklammert –, während § 98d StPO-E n.F. unbeanstandet blieb.⁴⁵

2. AG Reutlingen und die Verteidigungsperspektive

Dass diese Fragen nicht nur auf der Ebene der Eingriffsermächtigung, sondern auch im gerichtlichen Verfahren relevant werden, zeigt der Beschluss des *AG Reutlingen* vom 24. April 2025.⁴⁶ Dort beruhte der Tatverdacht nahezu ausschließlich auf der Auswertung einer Videoaufnahme durch eine polizeiliche Gesichtserkennungssoftware. Das Gericht ordnete die Beiordnung eines Pflichtverteidigers nach § 140 Abs. 2 StPO an, weil die Verwertbarkeit und der Beweiswert des softwaregestützten Treffers erhebliche rechtliche und tatsächliche Schwierigkeiten aufwarfen.⁴⁷

Die Begründung ist für die weitere Debatte aufschlussreich. Das *AG Reutlingen* beanstandete, dass weder die eingesetzte Software noch die Referenzdatenbank oder die verwendeten Qualitätskriterien hinreichend transparent seien. Unter Rückgriff auf die Anforderungen der Rechtsprechung zur Wiedererkennung machte es deutlich, dass ein bloßes algorithmisches „Match“ nicht ohne weiteres die Qualität eines belastbaren Identifizierungsbeweises erreicht.⁴⁸ Die freie richterliche Beweiswürdigung nach § 261 StPO setzt eine nachvollziehbare, rational überprüfbare Tatsachengrundlage voraus; eine Blackbox-Entscheidung kann diese Grundlage gerade in Grenzfällen nicht ohne weiteres liefern.⁴⁹

⁴¹ Kunze, in: Chibanguza/Kuß/Stege, KI-Hdb, 2. Aufl. (2022), 2. Teil: § 9 Rn. 100-109; Hilgendorf/Härtlein, in: HK-KI-VO, Art. 5 Rn. 1, 45-48; Raue, in: BeckOK-KI-Recht, KI-VO Art. 5 Rn. 1-3, 82; Wendehorst, in: Martini, KI-VO, Art. 5 Rn. 139-141; EuGH, Urt. v. 6.10.2020 – C-623/17, Rn. 76 ff.

⁴² *BVerfG*, Urt. v. 16.2.2023 – 1 BvR 1547/19, 1 BvR 2634/20, Rn. 50, 62, 71; zur Übertragung auf die biometrische Gesichtserkennung Teichmann, NSTZ 2026, 457 (461 f.).

⁴³ BT-Drs. 21/6806, S. 18 f.; *BVerfG*, Urt. v. 16.2.2023 – 1 BvR 1547/19 u.a.; zu den Anforderungen an eine strafprozessuale Nachsteuerung Teichmann, HRRS 2026, 13 (17 ff., 26).

⁴⁴ *BVerfG*, Urt. v. 16.2.2023 – 1 BvR 1547/19 u.a., Rn. 91 ff., 150 f.

⁴⁵ BT-Drs. 21/6806, S. 26 f. (Stellungnahme des Bundesrates) und S. 28 (Gegenäußerung der Bundesregierung).

⁴⁶ *AG Reutlingen*, Beschl. v. 24.4.2025 – 5 Ds 29 Js 1276/25; zur Einordnung Teichmann, ZfStw 2026, 221 (229 f.); ders., NJOZ 2026, 705 (708 f.).

⁴⁷ Willnow, in: KK-StPO, § 140 Rn. 28-29; Kämpfer/Travers, in: MüKo-StPO, § 140 Rn. 35-36; Krawczyk, in: BeckOK-StPO, § 140 Rn. 27-38; von Stetten, in: MAH Strafverteidigung, § 16 Rn. 22-30.

⁴⁸ BGH, Urt. v. 17.3.2021 – 5 StR 148/20 Rn. 11; BGH, NSTZ-RR 2017, 183 (184).

⁴⁹ Bartel, in: MüKo-StPO, § 261 Rn. 5-8, 139; Tiemann, in: KK-StPO, § 261 Rn. 5-10, 149; Eschelbach, in: BeckOK-StPO, § 261 Rn. 13-14.4; Murmann, in: NK-StPO, 2025, § 261 Rn. 62, 87-91; Brehmeier-Metz/Bröckers/Burghardt, in: HK-GS, 5. Aufl. (2022), § 261 Rn. 6-7; Roxin/Schünemann, Strafverfahrensrecht, 30. Aufl. (2022), § 24 Rn. 37 ff.

Der Beschluss belegt damit zweierlei. Erstens kann die fehlende normative und technische Transparenz den Einsatz der Gesichtserkennung schon im Zwischenverfahren zu einem Verteidigungsthema ersten Ranges machen. Zweitens trägt die bisweilen zu hörende Qualifikation des Softwaretreffers als bloßer „Ermittlungsansatz“ nicht, wenn auf ihm der gesamte Tatverdacht aufbaut. Wo die Maschine die Personenauswahl faktisch vorstrukturiert, muss das Strafverfahren diese Vorstrukturierung offenlegen und kontrollierbar machen.

VI. Folgerungen für einen neuen § 98d StPO

1. Was nicht geregelt werden darf

Die erste Folgerung ist negativ, aber zentral: Ein künftiger § 98d StPO darf den Abgleich mit biometrischen Datenbanken, die durch ungezieltes Auslesen von Bildern aus dem Internet oder von Überwachungsaufnahmen erstellt wurden, nicht erlauben.⁵⁰ Es handelt sich hierbei nicht um eine Frage bloßer Verhältnismäßigkeitsabstufung, sondern um eine unionsrechtliche Sperre. Eine nationale Ermächtigung, die private oder staatliche Internetdatenbanken dieser Art nutzbar machen wollte, stünde im Widerspruch zu Art. 5 Abs. 1 UAbs. 1 lit. e KI-VO.

Kriminalpolitisch mag das unbefriedigend erscheinen, weil gerade der Fall *Klette* die Ermittlungswirksamkeit solcher Suchen plastisch gemacht hat. Rechtsstaatlich folgt daraus jedoch kein Anpassungsdruck des Täterbegriffs oder der Eingriffsbefugnisse, sondern die schlichte Einsicht, dass nicht jede technisch mögliche Fahndungsmethode in den Werkzeugkasten des Strafverfahrensrechts übernommen werden darf.⁵¹ Die KI-VO zwingt den Gesetzgeber gerade dazu, zwischen zulässiger Ermittlungsinnovation und unionsrechtlich gesperrter biometrischer Masseninfrastruktur zu unterscheiden.

Diese Aussage lässt sich exemplarisch am § 98d StPO-E n.F. in der Fassung des Regierungsentwurfs verdeutlichen. Die in § 98d Abs. 1 StPO-E n.F. verwendete Formulierung „im Internet öffentlich zugängliche biometrische Daten“ ist hinsichtlich der Datenbasis unterbestimmt; sie erfasst nach dem Willen des Entwurfsverfassers ausdrücklich auch Daten aus sozialen Medien.⁵² Die Begründung versucht das unionsrechtliche Problem auf zwei Ebenen zu entschärfen – durch die Löschpflicht in Abs. 3 und durch die enge, an den Kommissionsleitlinien orientierte Auslegung des Art. 5 Abs. 1 UAbs. 1 lit. e KI-VO. Beide Wege verfehlen den Verbotszweck. Die Löschpflicht setzt erst nach der unionsrechtlich verbotenen Datenbankerstellung an; auch die anlassbezogen aufgebaute, anschließend gelöschte biometrische Suchdatenbank erfüllt den Tatbestand der „Erstellung oder Erweiterung“.⁵³ Die Verengung des Verbots auf Scraping unter

Einsatz von KI-Systemen würde es bei prozeduralem Auslesen ohne KI leerlaufen lassen, obwohl das funktionale Ergebnis identisch wäre.

Hinzu kommt der vom Entwurf selbst eröffnete Pfad zur mittelbaren Verwendung von Datenbanken, deren Aufbau gegen Art. 5 Abs. 1 UAbs. 1 lit. e KI-VO verstößt: Über die in der Begründung zu Abs. 3 angekündigte BKAG-Begleitnovelle und über die justizielle Rechtshilfe nach §§ 77d ff. IRG soll die Inanspruchnahme privater Anbieter in Drittstaaten ermöglicht werden.⁵⁴ Damit würde das deutsche Strafverfahren das Ergebnis einer unionsrechtlich verbotenen Praktik nachnutzen. Da der Verbotstatbestand neben dem Inverkehrbringen und der Inbetriebnahme auch die Verwendung erfasst, wird dieses Ergebnis nicht durch die Verlagerung der Datenbankerstellung ins Ausland legalisiert.

2. Was geregelt werden kann

Legalisierbar ist demgegenüber ein streng begrenzter Abgleich gegen polizeiliche Referenzdatenbanken. Ein solcher Abgleich beruht nicht auf dem Aufbau neuer, aus dem offenen Internet gespeister biometrischer Datenbanken, sondern auf bereits vorhandenen behördlichen Beständen.⁵⁵ Auch insoweit ist der Gesetzgeber allerdings an die Anforderungen der KI-VO, des JI-Datenschutzrechts und des Grundgesetzes gebunden.

Ein unions- und verfassungskonformer § 98d StPO müsste deshalb mindestens sieben Elemente enthalten: Erstens bedarf es einer eigenständigen, bereichsspezifischen Eingriffsnorm. Zweitens ist die Maßnahme auf einen abschließenden Katalog besonders schwerer Straftaten zu begrenzen. Drittens darf sie nur subsidiär eingesetzt werden, wenn andere Ermittlungsmaßnahmen wesentlich weniger Erfolg versprechen oder aussichtslos sind. Viertens ist grundsätzlich eine vorherige richterliche Anordnung erforderlich. Fünftens muss jeder Treffer vor weiterer Nutzung fachkundig manuell verifiziert werden; weder weitere Ermittlungsmaßnahmen noch Beweisverwertung dürfen auf einem unverifizierten Softwareergebnis beruhen. Sechstens sind Bias-Kontrollen, Dokumentationspflichten und technische Schutzmaßnahmen normativ vorzusehen. Siebtens bedarf es einer nachträglichen Benachrichtigung der Betroffenen sowie einer parlamentarischen Berichtspflicht.

Die strafprozessuale Architektur muss also an zwei Stellen zugleich ansetzen, und zwar bei der Eingriffsschwelle und bei der Ergebnisverwendung. Eine Norm, die nur den Abruf erlaubt, aber die Frage der menschlichen Kontrolle und der prozessualen Anschlussverwendung offenlässt, bliebe unvollständig. Umgekehrt genügt es nicht, nur Be-

⁵⁰ Verordnung (EU) 2024/1689, Art. 5 Abs. 1 lit. e; *Raue*, in: BeckOK-KI-Recht, KI-VO Art. 5 Rn. 82-88; *Hilgendorf/Härtlein*, in: HK-KI-VO, Art. 5 Rn. 45-48; *Wendehorst*, in: Martini, KI-VO, Art. 5 Rn. 139-141; *Lewandowski* (Fn. 13); Deutscher Bundestag (Fn. 13), S. 6-10.

⁵¹ Bundesnetzagentur (Fn. 14); Europäische Kommission (Fn. 14).

⁵² BT-Drs. 21/6806, S. 16.

⁵³ BT-Drs. 21/6806, S. 17; *Raue*, in: BeckOK-KI-Recht, KI-VO Art. 5 Rn. 82-88; *Wendehorst*, in: Martini, KI-VO, Art. 5 Rn. 139-141; *Hilgendorf/Härtlein*, in: HK-KI-VO, Art. 5 Rn. 45-48; Verordnung (EU) 2024/1689, ErwGr. 17, 32.

⁵⁴ BT-Drs. 21/6806, S. 17.

⁵⁵ BKA (Fn. 4); *Rückert*, StV 2025, 350 (356); zu den Mindestanforderungen an eine solche Norm *Teichmann*, ZfStw 2026, 221 (230 f.); *ders.*, NSZ 2026, 457 (462).

weisverwertungsfragen zu adressieren, solange die Erhebungsmaßnahme selbst auf einer unbestimmten oder unionsrechtswidrigen Grundlage beruht.

Der Regierungsentwurf enthält durchaus Elemente, die in eine verfassungs- und unionsrechtskonforme Regelung einzustellen wären. Zu nennen sind insbesondere der ausdrückliche Ausschluss des Echtzeitabgleichs (§ 98d Abs. 1 S. 2 StPO-E n.F.), die Protokollierungspflicht (§ 98d Abs. 2 StPO-E n.F.), die strikte Zweckbindung und Löschpflicht einschließlich der Templates (§ 98d Abs. 3 StPO-E n.F.) sowie die Aufnahme in den Katalog der Benachrichtigungspflichten nach § 101 Abs. 4 S. 1 Nr. 1a StPO-E n.F.⁵⁶ Diese Bausteine sind in einen unions- und verfassungskonformen Regelungsentwurf zu übernehmen – wobei die Löschpflicht zwar einen wichtigen datenschutzrechtlichen Schutzbeitrag leistet, die unionsrechtliche Sperre des Art. 5 Abs. 1 UAbs. 1 lit. e KI-VO indes nicht heilen kann.

Hinzutreten müssen daher: Erstens eine eindeutige Beschränkung auf polizeiinterne Referenzdatenbestände unter ausdrücklichem Ausschluss jeglicher Anbindung an scraping-basierte Internetdatenbanken – auch über den Weg der justiziellen oder polizeilichen Rechtshilfe an Drittstaatsanbieter. Zweitens ein Richtervorbehalt nach dem Vorbild des § 100e StPO, also Richter im Regelfall, Staatsanwaltschaft in Eilfällen, anstelle des im Entwurf vorgesehenen abgesenkten Anordnungsregimes. Drittens eine ausdrückliche Pflicht zur fachkundig-manuellen Trefferverifikation im Wortlaut des § 98d StPO selbst und nicht lediglich im Verweis auf Art. 14 Abs. 5 KI-VO. Viertens eine normierte Bias-Kontrolle, wie sie für die verfahrensübergreifende Datenanalyse in § 98e Abs. 4 S. 5 StPO-E n.F. bereits vorgesehen ist.

3. Normprogramm und kriminalpolitische Einordnung

Normtechnisch spricht vieles dafür, eine Vorschrift in der Nähe der §§ 98a ff. StPO zu verorten, ohne sich in die Logik der klassischen Rasterfahndung zurückzuziehen. Der gesetzliche Kern müsste lauten, dass bei Verdacht einer Katalogtat die Identität einer Person durch automatisierten Abgleich biometrischer Daten mit in polizeilichen Informationssystemen gespeicherten Referenzdaten festgestellt werden darf, sofern die Maßnahme subsidiär ist, richterlich angeordnet wird und jeder Treffer vor weiterer Verwendung manuell verifiziert wird. Ergänzend müssten Diskriminierungsprüfungen, Dokumentation, Benachrichtigung und der ausdrückliche Ausschluss internetbasierter biometrischer Datenbanken geregelt werden.

Kriminalpolitisch liegt darin kein technikfeindlicher Minimalismus. Der Gesetzgeber wäre weiterhin in der Lage, das reale Ermittlungsinteresse an einer Identifizierung unbekannter Beschuldigter zu berücksichtigen. Verwehrt bliebe ihm lediglich der Schritt in eine Architektur biometrischer Massenerschließung des offenen Netzes. Gerade diese Begrenzung ist aber keine Schwäche, sondern die eigentliche rechtsstaatliche Leistung einer künftigen Norm.

VII. Ergebnis

Die Debatte über KI-gestützte Gesichtserkennung im Strafverfahren darf nicht entlang der schlichten Frage geführt werden, ob „nachträgliche“ Fernidentifizierung zugelassen werden soll. Entscheidend ist vielmehr, welcher Datenbestand die Maßnahme trägt. Der Abgleich gegen polizeiliche Referenzdatenbanken und der Abgleich gegen aus dem Internet ausgeschrappte biometrische Datenbanken unterscheiden sich unions-, datenschutz- und verfassungsrechtlich kategorial.

Hieraus folgt ein klares Ergebnis. Ein künftiger § 98d StPO kann unionsrechtskonform nur den streng begrenzten Abgleich gegen polizeiinterne Referenzdatenbestände erfassen. Der Rückgriff auf internetbasierte biometrische Datenbanken bleibt durch Art. 5 Abs. 1 UAbs. 1 lit. e KI-VO gesperrt. Zugleich zeigt der Beschluss des *AG Reutlingen*, dass jede gesetzgeberische Antwort auch die prozessuale Anschlussverwendung der Treffer in den Blick nehmen muss. Der Gesetzgeber steht daher nicht vor der Wahl zwischen Fortschritt und Grundrechtsschutz, sondern vor der Aufgabe, eine technikfähige, aber klar begrenzte Eingriffsnorm zu schaffen. Nur eine solche Regelung kann verhindern, dass sich die strafprozessuale Diskussion über Gesichtserkennung zwischen kriminalpolitischer Überbietungsrhetorik und normativer Leerstelle erschöpft.

Der Regierungsentwurf vom 29.4.2026 markiert gegenüber dem Sicherheitspaket-Entwurf 2024 punktuelle Schutzfortschritte – insbesondere in der Zweckbindung und Löschpflicht des § 98d Abs. 3 StPO-E n.F. – perpetuiert jedoch den in diesem Beitrag aufgezeigten systematischen Grundfehler. Er überlässt die entscheidende Frage nach dem Referenzdatenbestand letztlich dem Vollzug, eröffnet über Rechtshilfe und die parallel eingebrachte BKAG-Begleitnovelle den mittelbaren Zugriff auf scraping-basierte Drittanbieter-Datenbanken und verzichtet auf ein genuines strafprozessuales Schutzniveau, das über die unionsrechtliche Mindestschwelle des Art. 26 Abs. 10 KI-VO hinausginge. Die Regulationsasymmetrie zwischen § 98d und § 98e StPO-E n.F. – mit deutlich höherem Schutzniveau für die Datenanalyse – zeigt zugleich, dass der Gesetzgeber durchaus in der Lage wäre, die vom *BVerfG* und von der KI-VO vorgegebenen Maßstäbe auch für die biometrische Fernidentifizierung zu konkretisieren. Die Stellungnahme des Bundesrates, die § 98d StPO-E n.F. unbeanstandet lässt und für § 98e StPO-E n.F. sogar eine Erweiterung anmahnt, deutet nicht darauf hin, dass sich dies im parlamentarischen Verfahren ändern wird; die öffentliche Anhörung des Innenausschusses vom 21.9.2026 hat diesen Befund bestätigt. Während das Bundeskriminalamt, die Gewerkschaft der Polizei und ein Vertreter der richterlichen Praxis den biometrischen Internetabgleich als unersetzliches Ermittlungsinstrument begrüßten, warnte der Deutsche Anwaltverein vor einer uferlosen, weit über die gezielte Personenfahndung hinausgehenden Befugnis, und AlgorithmWatch bewertete die Entwürfe als unionsrechtswidrig – mit der auch hier

⁵⁶ BT-Drs. 21/6806, S. 7-9, 24 f.

vertretenen Begründung, dass ein Abgleich mit Internetbildern ohne eine mittels KI erstellte Datenbank technisch nicht umsetzbar ist und die vorgesehene Auslagerung an private Anbieter in Drittstaaten das Verbot des Art. 5 Abs. 1 UAbs. 1 lit. e KI-VO umgeht. Aus der Wissenschaft wurde die Regelung teils als sehr weitreichend und

mangels einschlägiger Judikatur verfassungsrechtlich kaum einschätzbar bezeichnet. Die unionsrechtliche Sperre ist damit im parlamentarischen Verfahren als Einwand angekommen; eine Antwort des Gesetzgebers steht aus.⁵⁷

⁵⁷ BT-Drs. 21/6806, S. 26-28; zur öffentlichen Anhörung des Innenausschusses am 21.9.2026 Deutscher Bundestag, Geteiltes Echo zur Stärkung digitaler Ermittlungsbefugnisse, hib 725/2026 v. 21.9.2026, online abrufbar unter: <https://www.bundestag.de/presse/hib/kurzmeldungen-1216758> (zuletzt abgerufen am 23.9.2026) – dort auch die wiedergegebenen Einschätzungen von *Link* (BKA), *Poitz* (GdP), *Schmidtke* (OLG Düsseldorf), *Kempgens* (DAV) und *Löffelmann*; die schriftlichen Stellungnahmen der Sachverständigen sind als Ausschussdrucksachen 21(4)214 A bis H dokumentiert, online abrufbar unter: <https://www.bundestag.de/dokumente/textarchiv/2026/kw39-pa-inneres-1206160> (zuletzt abgerufen am 23.9.2026); zur Unionsrechtswidrigkeit *Sombetzki/Vieth-Ditlmann*, Stellungnahme AlgorithmWatch v. 17.9.2026, Ausschussdrucksache 21(4)214 D, S. 4-6.