

Retrograde biometrische Fernidentifizierung und europäisches Strafverfahrensrecht KI-Verordnung, JI-Richtlinie und der deutsche Reformdiskurs als Fallstudie unionsrechtlicher Vorprägung

Von Rechtsanwalt Dr. iur. Dr. rer. pol. **Fabian Teichmann**, LL.M. (London), MBA (Oxford),
St. Gallen*

Der Beitrag entwickelt die These, dass die deutsche Debatte über retrograde biometrische Fernidentifizierung ihr unionsrechtliches Schlüsselproblem verfehlt: Nicht die Nachträglichkeit der Suche, sondern die Datengrundlage entscheidet. Art. 5 Abs. 1 lit. e KI-VO untersagt die Erstellung und Erweiterung gescrippter Gesichtsdatabanken ohne strafverfolgungsrechtliche Ausnahme; die Richtlinie (EU) 2016/680 und die §§ 45 ff. BDSG binden biometrische Verarbeitung an Gesetzlichkeit, strikte Erforderlichkeit und das Verbot ausschließlich automatisierter belastender Entscheidungen. HessenDATA, GRCh und EMRK verschärfen die Anforderungen. Regelungsfähig bleibt danach allein die eng umgrenzte nachträgliche Suche in geschlossenen, rechtmäßig erhobenen Beständen, für die der Beitrag sieben Mindestanforderungen und einen Formulierungsvorschlag entwickelt. Die internetweite biometrische Suche erweist sich demgegenüber als regelungsunfähig.

I. Einleitung

Die Debatte über KI-gestützte Gesichtserkennung in der Strafverfolgung wird in Deutschland noch immer zu stark als innerstaatliche Frage der Ermittlungszweckmäßigkeit geführt. Gerade der seit 2024/2025 entfaltete Reformdiskurs zeigt jedoch das Gegenteil: Wer über retrograde biometrische Fernidentifizierung im Strafverfahren spricht, bewegt sich nicht in einem normativ offenen nationalen Raum, sondern in einem unionsrechtlich vorgeprägten Mehrebenengefüge.¹

Dieses Gefüge ist dreifach strukturiert. Erstens zieht die KI-Verordnung² mit unmittelbar geltenden Verboten und Risikoregeln harte unionsrechtliche Außenlinien ein.³ Zweitens binden die Richtlinie (EU) 2016/680⁴ und ihre Umset-

zung in den §§ 45 ff. BDSG jede biometrische Datenverarbeitung an Gesetzlichkeit, strikte Erforderlichkeit, besondere Garantien und das Verbot ausschließlich automatisierter belastender Entscheidungen.⁵ Drittens bleiben die verfassungsrechtlichen Maßstäbe des Grundgesetzes, vor allem nach der hessenDATA-Entscheidung des Bundesverfassungsgerichts, für die strafprozessuale Eingriffsermächtigung maßgeblich.⁶

Der zentrale Befund dieses Beitrags lautet, dass die deutsche Diskussion ihr unionsrechtliches Schlüsselproblem erkennt. Der neuralgische Punkt liegt nicht primär in der nachträglichen Suche als solcher, sondern in der Datengrundlage. Ein automatisierter biometrischer Abgleich mit frei im Internet auffindbaren Bildern setzt funktional einen GesichtsindeX voraus, der durch massenhaftes Scraping erstellt oder fortlaufend erweitert wird. Genau diesen Vorgang untersagt Art. 5 Abs. 1 lit. e KI-VO grundsätzlich und ohne strafverfolgungsrechtliche Ausnahme.⁷

Damit wird der deutsche Reformdiskurs zur Fallstudie europäischen Strafverfahrensrechts. Die Frage ist nicht, ob der nationale Gesetzgeber Gesichtserkennung „irgendwie“ zulassen möchte. Die Frage ist, ob und in welchem Umfang unionsrechtlich überhaupt ein Regelungskorridor verbleibt. Dieser Beitrag arbeitet diesen Korridor aus. Im Mittelpunkt stehen die KI-Verordnung und die Richtlinie (EU) 2016/680

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 = ABl. EU Nr. L 119 v. 4.6.2016.

⁵ Art. 7, 8, 10, 11 RL (EU) 2016/680; *Braun*, in: Gola/Heckmann, DSGVO, BDSG, Kommentar, 3. Aufl. 2022, BDSG § 48 Rn. 4 ff., § 54 Rn. 1 ff.; *Schwichtenberg*, in: Kühling/Buchner, DS-GVO BDSG, Kommentar, 4. Aufl. 2024, BDSG § 48 Rn. 2 ff., § 54 Rn. 4 f.; *Frenzel*, in: Paal/Pauly (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, Kommentar, 4. Aufl. 2026, BDSG § 48 Rn. 3 ff., § 54 Rn. 1 ff.

⁶ BVerfG, Urt. v. 16.2.2023 – 1 BvR 1547/19, 1 BvR 2634/20 = NJW 2023, 1196; *Singelstein*, NStZ 2012, 593; *Koranyi/Singelstein*, NJW 2011, 124 (128).

⁷ ErwG 43, Art. 5 Abs. 1 lit. e VO (EU) 2024/1689; *Wendehorst*, in: Martini/Wendehorst (Hrsg.), Verordnung über künstliche Intelligenz, Kommentar, 2. Aufl. 2025, Art. 5 Rn. 139–141; *Hilgendorf/Härtlein* (Fn. 3), Art. 5 Rn. 45–47; *Raue*, in: Schefzig/Kilian (Fn. 3), KI-VO Art. 5 Rn. 82–88; *Lewandowski*, Braucht die Polizei eine Datenbank zum biometrischen Abgleich?, Das Durchsuchen von Internetbildern zur Gesichtserkennung, Technisches Gutachten, September 2025; Deutscher Bundestag, Fachbereiche EU 6 und WD 5, Biometrischer Abgleich mit Bildern aus dem Internet, Das technische Gutachten im Auftrag von AlgorithmWatch, S. 6 f.

* Der Autor ist Lehrbeauftragter an der Universität zu Köln, der Universität Kassel und der Universität Trier sowie Managing Partner einer Anwaltskanzlei.

¹ Vgl. Koalitionsvertrag von CDU, CSU und SPD für die 21. Legislaturperiode v. 5.5.2025, Z. 2635–2637, 2852; *Rückert*, StV 2025, 350.

² Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates v. 13.6.2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz = ABl. EU Nr. L 2024/1689.

³ Art. 2 Abs. 3, Art. 3 Nrn. 42–44, 5 Abs. 1 lit. e und h, 6 Abs. 2 (i.V.m. Anh. III Nr. 1 lit. a), 26 Abs. 10, 113 VO (EU) 2024/1689; *Hilgendorf/Härtlein*, Verordnung über künstliche Intelligenz, Handkommentar, 2025, Art. 2 Rn. 11, Art. 5 Rn. 45–48; *Voigt*, in: Schefzig/Kilian (Hrsg.), Beck'scher Online-Kommentar, KI-Recht, Stand: 1.11.2025, KI-VO Art. 2 Rn. 36–39.

⁴ Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates v. 27.4.2016 zum Schutz natürlicher Personen bei

sowie das BDSG; die deutsche Reformdebatte dient als Fallstudie, an der sich die unionsrechtliche Vorprägung nationaler Strafverfahrensgesetzgebung exemplarisch zeigen lässt.⁸

II. Begriffe, Technik und Einsatzformen

1. Politische und unionsrechtliche Terminologie

Der politische Begriff der „retrograden biometrischen Fernidentifizierung“ ist unscharf. Er beschreibt eine nachträgliche biometrische Suche in bereits vorhandenen Bildbeständen, sagt aber für sich genommen nichts darüber aus, ob die Suche in einem polizeiinternen Referenzsystem, in einem abgeschlossenen CCTV-Bestand oder im offenen Internet stattfindet. Gerade diese Unterscheidung ist rechtlich entscheidend.⁹

Die KI-Verordnung arbeitet mit anderen Begriffen. Sie unterscheidet zwischen einem Echtzeit-Fernbiometrie-System und einem System zur nachträglichen biometrischen Fernidentifizierung.¹⁰ Hinzu tritt die Definition des „öffentlich zugänglichen Ortes“ als physischer Ort, der einer unbestimmten Zahl natürlicher Personen zugänglich ist.¹¹ Bereits begrifflich zeigt sich damit, dass internetbasierte Gesichtssuche nicht deckungsgleich mit der unionsrechtlich besonders regulierten Konstellation der Echtzeitüberwachung öffentlich zugänglicher physischer Räume ist. Wer die Debatte dogmatisch sauber führen will, darf diese Kategorien nicht vermengen.

Gerade darin liegt ein Grundproblem des deutschen Reformdiskurses. Die politische Formel der „retrograden Fernidentifizierung“ nivelliert Konstellationen von höchst unterschiedlicher Eingriffsintensität und unterschiedlicher unionsrechtlicher Behandlung. Ein Abgleich eines Täterbildes mit einer rechtmäßig erhobenen, geschlossenen polizeilichen Referenzdatenbank wirft andere Fragen auf als die Suche in Milliarden im Internet ausgelesener Bilder. Die unionsrechtliche Bewertung entscheidet sich deshalb nicht am Schlagwort, sondern an Systemarchitektur und Datengrundlage.¹²

⁸ FRA, *Facial Recognition Technology: Fundamental Rights considerations in the context of law enforcement*, 2020, S. 2; EDPB, *Leitlinien 05/2022 über den Einsatz von Gesichtserkennungstechnologie im Bereich der Strafverfolgung*, Version 2.0, Angenommen am 26. April 2023, Ziff. 3; Rückert, StV 2025, 350.

⁹ Vgl. *Coombe/Roth-Isigkeit*, ZfDR 2024, 391.

¹⁰ Art. 3 Nrn. 42–43 VO (EU) 2024/1689; *Hilgendorf/Härtlein* (Fn. 3), Art. 3 Rn. 44–45.

¹¹ Art. 3 Nr. 44, ErwG 38 VO (EU) 2024/1689; *Wendehorst* (Fn. 7), Art. 3 Rn. 335–340; *Hilgendorf/Härtlein* (Fn. 3), Art. 3 Rn. 46; *Kirschke-Biller/Füllsack*, in: Schefzig/Kilian (Fn. 3), KI-VO Art. 3 Rn. 519.

¹² DSK, *Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder v. 20.9.2024*, abrufbar unter https://www.datenschutzkonferenz-online.de/media/en/2024-09-20_Entschliessung_DSK_Gesichtserkennung.pdf (22.6.2026); EDPB (Fn. 8), Ziff. 3.2.

2. Technische Grundstruktur

Moderne Gesichtserkennung arbeitet nicht mit einer bloß visuellen Ähnlichkeitssuche, sondern mit der Extraktion biometrischer Merkmalsvektoren. Aus einem Gesichtsbild wird ein sogenanntes face embedding gebildet, das mathematisch mit Referenzvektoren verglichen werden kann.¹³ Das Ergebnis ist regelmäßig kein Ja/Nein-Befund, sondern ein Wahrscheinlichkeits- oder Ähnlichkeitsscore, der von der Qualität des Ausgangsbildes, dem Referenzmaterial, dem Schwellwert des Systems und der Güte des Trainingsdatensatzes abhängt.¹⁴

Die rechtliche Relevanz dieser technischen Struktur ist erheblich. Erstens erklärt sie die gesteigerte Eingriffsintensität: Biometrische Daten sind nicht austauschbar wie Passwörter, sondern an die Person gebunden und praktisch dauerhaft kompromittierbar. Zweitens macht sie deutlich, dass eine Suchanfrage nur so gut ist wie ihr Referenzbestand. Drittens zeigt sie, dass der biometrische Treffer immer nur ein algorithmisch erzeugtes Ähnlichkeitsurteil ist, kein selbstinterpretierender Tatsachenbeweis.¹⁵

Diese technische Eigenart hat dogmatischen Eigenwert. Bereits die Erstellung des Embedding ist ein eigenständiger Eingriff in das Recht auf informationelle Selbstbestimmung; der Personenbezug folgt nicht erst aus der späteren Verknüpfung mit identifizierenden Daten, sondern bereits daraus, dass der Vektor eindeutig aus den körpergebundenen Merkmalen der betroffenen Person abgeleitet ist und dieser unmittelbar zugeordnet werden kann. Auch der Abgleich und das Auftauchen einer Person auf einer Kandidatenliste sind als jeweils eigenständige, kumulativ wirkende Eingriffe einzuordnen.¹⁶ Wer die rechtliche Bewertung biometrischer Fernidentifizierung am bloßen „Treffer“ festmacht, verkennt damit zwei Drittel der eingriffsrelevanten Vorgänge.

Hinzu kommt das bekannte Problem ungleicher Fehleraten. Die Genauigkeit sinkt bei schlechten Lichtverhältnissen, schrägen Blickwinkeln, veralteten Vergleichsbildern oder niedriger Auflösung; zugleich variieren Falschzuordnungen nach Hautfarbe, Geschlecht und Alter.¹⁷ Wer biometrische Fernidentifizierung normativ regeln will, muss deshalb nicht nur an die Eingriffsschwelle denken, sondern ebenso an Fehlerfolgen, Diskriminierungsrisiken und die Anforderungen an sachkundige menschliche Nachkontrolle.

¹³ *Hornung/Schindler*, ZD 2017, 203 (204); DSK, *Entschließung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder v. 30.3.2017*, abrufbar unter https://www.datenschutzkonferenz-online.de/media/en/20170330_en_gesichtserkennung.pdf (22.6.2026).

¹⁴ Vgl. NISTIR, *Face Recognition Vendor Test (FRVT) – Part 3: Demographic Effects*, abrufbar unter <https://nvlpubs.nist.gov/nistpubs/ir/2019/nist.ir.8280.pdf> (22.6.2026); FRA (Fn. 8), S. 9.

¹⁵ Vgl. EDPB (Fn. 8), S. 9; *Schindler*, CR 2023, 341.

¹⁶ *Hahn*, *Automatisierte Gesichtserkennung in der Strafverfolgung*, 2025, S. 96–99, 101–104.

¹⁷ NISTIR (Fn. 14); FRA (Fn. 8), S. 9.

3. Einsatzformen und Eingriffsintensität

Für das Strafverfahren lassen sich mindestens vier Konstellationen unterscheiden: erstens der Abgleich eines unbekannten Täterbildes mit einer geschlossenen polizeilichen Referenzdatenbank, etwa INPOL; zweitens die nachträgliche Suche in einem rechtmäßig gesicherten, räumlich und zeitlich abgegrenzten Bestand von Videoaufzeichnungen; drittens die Echtzeitlokalisierung in öffentlich zugänglichen Räumen; viertens die internetbasierte Suche in öffentlich zugänglichen Bildbeständen.¹⁸

Diese Konstellationen sind weder tatsächlich noch rechtlich gleichwertig. Der Abgleich mit einer geschlossenen polizeilichen Datenbank greift zwar tief ein, bleibt aber auf einen bereits vorhandenen, institutionell kontrollierten Referenzraum bezogen. Die nachträgliche Suche in einem bestimmten CCTV-Bestand kann – jedenfalls bei enger räumlich-zeitlicher Begrenzung – unionsrechtlich grundsätzlich denkbar sein, weil sie auf einen geschlossenen Datensatz rechtmäßig erhobener Aufnahmen zielt.¹⁹ Die Echtzeitidentifizierung in öffentlich zugänglichen Räumen ist demgegenüber wegen ihres permanenten Überwachungspotentials unionsrechtlich grundsätzlich verboten und nur ausnahmsweise zulässig.²⁰ Der Internetabgleich schließlich ist dogmatisch ein Sonderfall, da nicht die Zeitdimension, sondern die Datengrundlage hier das Hauptproblem ist.

Gerade der Internetabgleich darf deshalb nicht als bloße Unterart der nachträglichen Fernidentifizierung behandelt werden. Technisch setzt die automatisierte biometrische Suche im offenen Netz einen Index voraus, der Gesichter aus unterschiedlichsten Quellen extrahiert, strukturiert und suchbar macht. Der Sachstand des Deutschen Bundestages von Januar 2026 bestätigt insoweit den bereits im AlgorithmWatch-Gutachten herausgearbeiteten Befund, dass ein sinnvoller biometrischer Abgleich mit Bildern „aus dem Internet“ praktisch nicht ohne eine Datenbank zur Gesichtssuche auskommt.²¹ Die technische Vorfrage wird damit zur unionsrechtlichen Hauptfrage.

Die unterschiedliche Eingriffsintensität dieser Konstellationen lässt sich entlang einer kumulativen Faktorenanalyse präzise greifen. Hahn hat hierfür fünf Strukturmerkmale herausgearbeitet, deren Zusammentreffen das spezifische Gefährdungspotenzial automatisierter Gesichtserkennung in der Strafverfolgung ausmacht:²²

- Streubreite, weil die Maßnahme nicht den Beschuldigten, sondern hauptsächlich Unbeteiligte trifft
- Fehleranfälligkeit, weil biometrische Treffer typische Falschidentifikationsmuster aufweisen

- Heimlichkeit, weil die Betroffenen weder von der Erfassung noch vom Abgleich Kenntnis erlangen
- Vernetzungsmöglichkeit, weil der mathematisierte Merkmalsvektor mit beliebigen anderen Datenbeständen verknüpfbar ist
- Biometrie, also die Anknüpfung an unwiderruflich personengebundene Körpermerkmale

Diese Faktorenanalyse verdient hier Beachtung, weil sie zugleich eine Prüfungsmatrix für die unionsrechtliche und strafprozessuale Bewertung jeder konkreten Einsatzform liefert. Je mehr dieser Faktoren in einer Konstellation kumulieren – so der Internetabgleich, der alle fünf maximiert –, desto enger wird der unionsrechtliche Korridor.

III. Der unionsrechtliche Ordnungsrahmen

1. Die KI-Verordnung als negativ und prozedural harmonisierendes Regime

Die KI-Verordnung gilt grundsätzlich auch für die Strafverfolgung. Ihre Bereichsausnahme für die nationale Sicherheit greift für die gewöhnliche polizeiliche und staatsanwaltschaftliche Verfolgung von Straftaten nicht ein.²³ Zugleich ordnet die Verordnung selbst an, dass sie die Anwendung des Datenschutzrechts, insbesondere der Richtlinie (EU) 2016/680, unberührt lässt.²⁴ Für das Strafverfahren bedeutet dies, dass die KI-Verordnung keine Eingriffsermächtigung ersetzt, sondern der nationalen Gesetzgebung unionsrechtliche Schranken und Mindestanforderungen setzt.

Dogmatisch handelt es sich um ein asymmetrisches Harmonisierungsregime. Die Verordnung harmonisiert weder den Anfangsverdacht noch die strafprozessuale Beweislehre umfassend. Sie bestimmt aber, welche Systeme überhaupt eingesetzt werden dürfen, welche Systeme als Hochrisiko-Systeme gelten, welche Autorisierung für bestimmte Einsatzformen erforderlich ist und in welchen Punkten die Mitgliedstaaten nur strenger, nicht aber großzügiger sein dürfen.²⁵ In diesem Sinne prägt die KI-Verordnung ein europäisches Strafverfahrensrecht nicht als einheitliches Kodexrecht, wohl aber als System negativer Verbote und prozeduraler Bindungen.

Für die nationale Gesetzgebung folgt daraus ein doppelter Legalisierungstest. Eine biometrische Ermittlungsmaßnahme ist nur dann zulässig, wenn sie erstens auf einer hinreichend bestimmten innerstaatlichen Eingriffsnorm beruht und zweitens innerhalb des unionsrechtlich eröffneten Korridors verbleibt. Das ist mehr als ein bloßes Anwendungsvorrangproblem. Die nationale Norm selbst muss so gefasst sein, dass ihr Anwendungsbereich nicht in Konstellationen hineinreicht, die die KI-Verordnung sperrt.²⁶

¹⁸ Coombe/Roth-Isigkeit, ZfDR 2024, 391.

¹⁹ ErwG 95 VO (EU) 2024/1689; Hilgendorf/Härtlein (Fn. 3), Art. 26 Rn. 14–15; Dengä, in: Schefzig/Kilian (Fn. 3), KI-VO Art. 26 Rn. 86–87.

²⁰ Art. 5 Abs. 1 lit. h sublit. ii und iii VO (EU) 2024/1689; Raue (Fn. 7), KI-VO Art. 5 Rn. 140–145, 146–149; Hilgendorf/Härtlein (Fn. 3), Art. 5 Rn. 82–94.

²¹ Deutscher Bundestag (Fn. 7), S. 6 f.; Lewandowski (Fn. 7).

²² Hahn (Fn. 16), S. 30 ff., 121 ff.

²³ Art. 2 Abs. 3 VO (EU) 2024/1689; Voigt (Fn. 3), KI-VO Art. 2 Rn. 36–39; Hilgendorf/Härtlein (Fn. 3), Art. 2 Rn. 11.

²⁴ Art. 2 Abs. 7, ErwG 95 VO (EU) 2024/1689; Voigt (Fn. 3), KI-VO Art. 2 Rn. 48.

²⁵ Art. 5 Abs. 5, 26 Abs. 7, Abs. 10, 113 lit. a VO (EU) 2024/1689; Dengä (Fn. 19), KI-VO Art. 26 Rn. 107–108.

²⁶ Martini, NVwZ Extra 1–2/2022, 1 (9 f.).

2. Art. 5 Abs. 1 lit. e KI-VO: das Verbot gescrapter Gesichtssindizes

Art. 5 Abs. 1 lit. e KI-VO verbietet das Inverkehrbringen, die Inbetriebnahme und die Verwendung von KI-Systemen zur Erstellung oder Erweiterung von Gesichtserkennungsdatenbanken durch ungezieltes Auslesen von Gesichtsbildern aus dem Internet oder von Videoüberwachungsanlagen.²⁷ Erwägungsgrund 43 begründet dieses Verbot mit den massiven Gefahren für Privatheit und Datenschutz, die aus der flächendeckenden biometrischen Indexierung unbeteiligter Personen entstehen.²⁸ Auffällig und für die Strafverfolgung entscheidend ist das Fehlen jeder strafprozessualen Ausnahme. Anders als Art. 5 Abs. 1 lit. h KI-VO enthält lit. e keinen Öffnungstatbestand für schwere Straftaten, richterliche Anordnungen oder Gefahrenlagen.

Damit steht fest: Der unionsrechtliche Gesetzgeber hat die Erstellung und Erweiterung gescrapter Gesichtssindizes als solche normativ disqualifiziert. Nationale Strafverfolgungsgesetzgebung kann diese Bewertung nicht relativieren. Sie kann insbesondere nicht dadurch umgangen werden, dass sie statt von der Erstellung einer Gesichtserkennungsdatenbank neutraler von einem „Abgleich mit öffentlich zugänglichen Daten“ spricht. Wo die technische Funktionsfähigkeit der Maßnahme einen nach Art. 5 Abs. 1 lit. e KI-VO verbotenen Index voraussetzt, ist die Maßnahme unionsrechtlich gesperst.²⁹

Das ist der dogmatische Schlüssel für die Bewertung des Internetabgleichts. Selbst wenn man begrifflich argumentierte, dass eine internetgestützte Suche nicht unter das Echtzeitverbot des Art. 5 Abs. 1 lit. h KI-VO fällt, weil Online-Räume keine öffentlich zugänglichen physischen Orte sind, bliebe lit. e als selbständige Sperre bestehen. Der Versuch, internetbasierte biometrische Suche unionsrechtlich über die Hintertür des nationalen Strafprozessrechts zu legalisieren, scheitert daher an der Datengrundlage.³⁰

Freilich muss dogmatisch sauber unterschieden werden. Art. 5 Abs. 1 lit. e KI-VO verbietet nicht jede Nutzung eines einzelnen öffentlich zugänglichen Bildes im Ermittlungsverfahren. Erfasst ist vielmehr die systematische biometrische Datenbankbildung durch ungezieltes Scraping. Gerade für die politisch diskutierte automatisierte Gesichtssuche im offenen Internet ist aber diese Datenbankbildung funktional konstitutiv. Deshalb bleibt für eine gesetzgeberische Freigabe der internetweiten biometrischen Suche kein realistischer unionsrechtlicher Raum.³¹

²⁷ Art. 5 Abs. 1 lit. e, ErwG 43 VO (EU) 2024/1689; Hilgendorf/Härtlein (Fn. 3), Art. 5 Rn. 45–48.

²⁸ ErwG 43 VO (EU) 2024/1689; Raue (Fn. 7), KI-VO Art. 5 Rn. 82.

²⁹ So bereits Lewandowski (Fn. 7); Deutscher Bundestag (Fn. 7), S. 6 f.; Wendehorst (Fn. 7), Art. 5 Rn. 139–141; Hilgendorf/Härtlein (Fn. 3), Art. 5 Rn. 45–48.

³⁰ Bundesnetzagentur, Verbotene Praktiken, abrufbar unter https://www.bundesnetzagentur.de/DE/Fachthemen/Digitales/KI/8_VerbotenePraktiken/start.html (22.6.2026).

³¹ Martini/Kemper, CR 2023, 341.

3. Art. 5 Abs. 1 lit. h KI-VO: Echtzeitidentifizierung in öffentlich zugänglichen Räumen

Von lit. e zu trennen ist Art. 5 Abs. 1 lit. h KI-VO. Danach ist die Verwendung von Echtzeit-Fernbiometrie-Systemen in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken grundsätzlich verboten.³² Ausnahmen bestehen nur in eng umgrenzten Konstellationen, etwa zur Suche nach Opfern bestimmter schwerer Delikte, zur Abwehr einer konkreten terroristischen Bedrohung oder zur Lokalisierung bestimmter Verdächtiger bei schweren Straftaten; hinzu treten eine vorgängige richterliche oder administrative Genehmigung und weitere Verhältnismäßigkeitsanforderungen.³³

Für den hier interessierenden Internetabgleich ist diese Norm jedoch nur mittelbar relevant. Gerade weil „öffentlich zugängliche Orte“ im unionsrechtlichen Begriffsverständnis physische Orte sind, taugt Art. 5 Abs. 1 lit. h KI-VO nicht als dogmatischer Anker zur Legalisierung oder Illegalisierung internetbasierter Suchvorgänge. Die unionsrechtliche Auseinandersetzung um das Internet wird von lit. e entschieden, nicht von lit. h.³⁴ Der häufig anzutreffende Verweis auf das Echtzeitverbot geht deshalb am Kern vorbei, wenn es um die nachträgliche Suche in gescraptern Web-Bildbeständen geht.

Gleichwohl ist lit. h für den deutschen Reformdiskurs wichtig, weil er zeigt, wie restriktiv die KI-Verordnung gerade bei massenüberwachungsnahen biometrischen Einsatzformen verfährt. Dies bestätigt den unionsrechtlichen Grundentscheid gegen entgrenzte biometrische Fernüberwachung und spricht systematisch dagegen, den Internetabgleich als rechtlich weniger problematisch zu behandeln, nur weil er nicht im physischen Raum stattfindet.³⁵

4. Nachträgliche Fernidentifizierung, Hochrisiko-Einstufung und Art. 26 Abs. 10 KI-VO

Biometrische Fernidentifizierungssysteme sind als Hochrisiko-KI-Systeme eingestuft.³⁶ Damit greifen die bekannten Anforderungen an Risikomanagement, Daten- und Daten-Governance, technische Dokumentation, Protokollierung, Transparenz und menschliche Aufsicht.³⁷ Für das Strafverfahren bedeutet dies nicht nur technische Compliance. Die Anforderungen schlagen auf die prozessuale Ausgestaltung durch.

³² Art. 5 Abs. 1 lit. h VO (EU) 2024/1689; Hilgendorf/Härtlein (Fn. 3), Art. 5 Rn. 67.

³³ Art. 5 Abs. 2–4 VO (EU) 2024/1689; vgl. Hilgendorf/Härtlein (Fn. 3), Art. 5 Rn. 67, 78, 79; Wendehorst (Fn. 7), Art. 5 Rn. 206–216.

³⁴ Art. 3 Nr. 44 VO (EU) 2024/1689; Hilgendorf/Härtlein (Fn. 3), Art. 3 Rn. 46; Wendehorst (Fn. 7), Art. 3 Rn. 335–340.

³⁵ Vgl. ErwG 32, 38 und 95 VO (EU) 2024/1689; FRA (Fn. 8), S. 1; EDPB (Fn. 8), Ziff. 3.1–3.2.

³⁶ Art. 6 Abs. 2 i.V.m. Anh. III Nr. 1 lit. a VO (EU) 2024/1689; Klawonn, in: Schefzig/Kilian (Fn. 3), Art. 6 Rn. 16–18.

³⁷ Art. 9–14 VO (EU) 2024/1689; Klawonn (Fn. 36), KI-VO Art. 6 Rn. 16–18; Gerdemann, in: Schefzig/Kilian (Fn. 3), KI-VO Art. 9 Rn. 16–31; Kilian/Schefzig, in: Schefzig/Kilian (Fn. 3), KI-VO Art. 10 Rn. 16–20; Zech/Linhart, in: Schefzig/Kilian (Fn. 3), KI-VO Art. 13 Rn. 16–25; Buchner, in: Schefzig/Kilian (Fn. 3), KI-VO Art. 14 Rn. 33–37.

Eine Strafprozessordnung, die den Einsatz zwar erlaubt, aber keine Vorkehrungen für Protokollierung, Qualitätskontrolle und menschliche Nachprüfung trifft, bleibt rechtsstaatlich unvollständig.

Hinzu kommt Art. 26 Abs. 10 KI-VO. Die Norm regelt speziell die Verwendung von Systemen zur nachträglichen biometrischen Fernidentifizierung für Strafverfolgungszwecke. Sie verlangt grundsätzlich eine vorherige richterliche oder administrative Genehmigung, lässt nur eng begrenzte Eilkonstellationen zu, untersagt ungezielte Nutzung und bestimmt ausdrücklich, dass Entscheidungen mit nachteiliger Rechtswirkung nicht allein auf der Ausgabe des Systems beruhen dürfen.³⁸ Bereits Erwägungsgrund 95 ist für die nationale Dogmatik aufschlussreich, indem er eine zulässige nachträgliche Suche als zielgerichtet, notwendig, verhältnismäßig und auf einen geschlossenen Datensatz rechtmäßig erlangten Videomaterials bezogen beschreibt.³⁹

Gerade diese Passage verdient größere Beachtung. Sie macht deutlich, dass die KI-Verordnung für zulässige *ex-post*-Suchformen von „closed datasets“ ausgeht, nicht von offenen, durch Scraping generierten Megadatenbanken. Das unionsrechtliche Modell ist also die eng begrenzte, fallbezogene Nachsuche in rechtmäßig erhobenen Beständen, und nicht die internetweite biometrische Suchmaschine. Die deutsche Reformdebatte muss sich daran messen lassen.⁴⁰

Schließlich ist hervorzuheben, dass Art. 26 Abs. 10 KI-VO und die Hochrisiko-Regeln keine nationale Eingriffsnorm substituieren. Sie setzen deren unionsrechtlichen Rahmen. Daraus folgt zugleich eine wichtige dogmatische Konsequenz: Wo die Strafprozessordnung keine besondere Eingriffsermächtigung und keine verfahrensrechtliche Umsetzung menschlicher Kontrolle, Dokumentation und Verteidigungszugänglichkeit enthält, wird der unionsrechtliche Rahmen nicht bloß „ergänzt“, sondern praktisch unterlaufen.⁴¹

Wie weit das Verbot ausschließlich systembasierter Entscheidungen nach Art. 26 Abs. 10 UAbs. 3 S. 2 KI-VO reicht, ist im Schrifttum noch nicht abschließend geklärt. Der Wortlaut „ausschließlich auf der Grundlage“/„based solely on“ ist parallel zu Art. 11 II-RL und Art. 22 DSGVO auszulegen. Eine Entscheidung erfolgt jedenfalls dann ausschließlich automatisiert, wenn ein Mensch das Ergebnis nur „abnickt“ und ohne inhaltliche Prüfung formal bestätigt. Dasselbe gilt, wenn sich die menschliche Beteiligung auf das Herausfiltern offensichtlich unplausibler Vorschläge beschränkt. Im grundrechtssensiblen Bereich der Strafverfolgung ist daher eine echte inhaltliche Kontrolle durch mehr als eine fachlich qualifizierte Person zu fordern, die zudem die rechtliche Kompetenz zur abweichenden Entscheidung besitzt.⁴² Übertragen auf die biometrische Fernidentifizierung bedeutet

dies: Die Verifikation muss durch geschulte Lichtbildsachverständige erfolgen, die Funktionsweise, Fehlerraten und systematische Verzerrungen des konkret verwendeten Systems verstehen. Eine bloß stichprobenartige oder rein formale Bestätigung genügt nicht. Damit erweist sich das oft beschworene „human in the loop“ als unzureichend, soweit es nicht durch verfahrensrechtliche Qualifikations-, Dokumentations- und Unabhängigkeitsanforderungen unterfüttert wird.

IV. Richtlinie (EU) 2016/680, BDSG und Grundrechte

1. Gesetzlichkeit und Bestimmtheit nach Art. 8 RL (EU) 2016/680

Neben der KI-Verordnung prägt die Richtlinie (EU) 2016/680 das unionsrechtliche Strafverfahrensrecht. Art. 8 der Richtlinie erlaubt die Verarbeitung personenbezogener Daten durch zuständige Behörden nur, wenn sie für die Wahrnehmung einer entsprechenden Aufgabe erforderlich ist und auf Unionsrecht oder mitgliedstaatlichem Recht beruht; dieses Recht muss jedenfalls Verarbeitungszwecke, Datenkategorien und Zielsetzungen hinreichend bestimmen.⁴³ Der deutsche Gesetzgeber hat diese Anforderungen in den §§ 45 ff. BDSG umgesetzt.⁴⁴

Für die Diskussion um biometrische Fernidentifizierung ist das von erheblicher Tragweite. Das unionsrechtliche Gesetzlichkeitsgebot bestätigt und verstärkt den innerstaatlichen Bestimmtheits- und Wesentlichkeitsgedanken. Eine bloße Rückgriffsermächtigung auf die Generalklauseln der §§ 161, 163 StPO genügt deshalb nicht nur verfassungsrechtlich kaum, sondern steht auch unter unionsrechtlichem Druck. Je sensibler die Datenkategorie und je höher die Eingriffsintensität, desto genauer muss die gesetzliche Grundlage die zulässigen Zwecke, Datensätze, Zugangsvoraussetzungen und Sicherungen konturieren.⁴⁵

Damit gewinnt die Frage nach der bereichsspezifischen Eingriffsnorm eine unionsrechtliche Zusatzdimension. Sie ist nicht nur Ausdruck nationaler Verfassungsdogmatik, sondern unionsrechtliche Pflicht. Gerade darin zeigt sich die Vorprägung nationaler Strafverfahrensautonomie: Der nationale Gesetzgeber bleibt frei in der konkreten Ausgestaltung, aber nicht frei darin, überhaupt mit einer offenen Generalermächtigung zu operieren.⁴⁶

2. Strikte Erforderlichkeit biometrischer Verarbeitung: Art. 10 RL (EU) 2016/680 und § 48 BDSG

Biometrische Daten zur eindeutigen Identifizierung einer Person gehören zu den besonders sensiblen Datenkategorien. Art. 10 RL (EU) 2016/680 erlaubt ihre Verarbeitung nur, wenn sie strikt erforderlich ist, angemessenen Garantien unterliegt und durch Gesetz zugelassen oder ausnahmsweise aus ande-

³⁸ Art. 26 Abs. 1–6, Abs. 10 VO (EU) 2024/1689; *Hilgendorf/Härtlein* (Fn. 3), Art. 26 Rn. 14–15; *Denga* (Fn. 19), KI-VO Art. 26 Rn. 77, 88–106.

³⁹ *Hilgendorf/Härtlein* (Fn. 3), Art. 26 Rn. 15.

⁴⁰ Vgl. *Eisenberger/Binder*, in: *Martini/Wendehorst* (Fn. 7), Art. 26 Rn. 68–77.

⁴¹ *Eisenberger/Binder* (Fn. 40), Art. 26 Rn. 68–77.

⁴² *Hahn* (Fn. 16), S. 184–187.

⁴³ Art. 8 Abs. 1–2 RL (EU) 2016/680.

⁴⁴ Vgl. *Wolff/v. Ungern-Sternberg*, in: *Wolff/Brink/v. Ungern-Sternberg* (Hrsg.), *Beck'scher Online-Kommentar, Datenschutzrecht*, Stand: 1.11.2025, BDSG § 45 Rn. 4; *Braun* (Fn. 5), BDSG § 45 Rn. 1–4.

⁴⁵ DSK (Fn. 12); *Martini, NVwZ Extra 1–2/2022*, 1 (10 f.).

⁴⁶ *Coombe/Roth-Isigkeit, ZfDR 2024*, 391 (401 ff.).

ren in der Norm genannten Gründen gerechtfertigt ist.⁴⁷ § 48 BDSG konkretisiert dies innerstaatlich und verlangt geeignete Garantien zum Schutz der Rechte und Freiheiten der betroffenen Person.⁴⁸

Die Verwendung der „strikten Erforderlichkeit“ ist für die biometrische Fernidentifizierung von größerer dogmatischer Schärfe als die gewöhnliche Verhältnismäßigkeitsformel. Sie verlangt nicht nur eine abstrakt nützliche Technik, sondern eine auf den konkreten Ermittlungszweck bezogene Unverzichtbarkeit oder jedenfalls eine sehr enge funktionale Notwendigkeit. Daraus folgen mehrere Konsequenzen, und zwar, dass die Datengrundlage begrenzt, der Suchraum fallbezogen, die Maßnahme subsidiär und die Speicher- sowie Zugriffsgestaltung besonders abgesichert sein muss.⁴⁹ Ein offener, anlasslos erweiterbarer Internetindex ist mit diesem Maßstab ersichtlich unvereinbar.

Besonders instruktiv ist in diesem Zusammenhang ein verbreitetes Fehlargument. Weil Bilder im Internet öffentlich zugänglich seien, dürften sie auch biometrisch ausgewertet werden. Art. 10 RL (EU) 2016/680 widerlegt diese Verkürzung. Selbst dort, wo Daten von der betroffenen Person öffentlich gemacht wurden, folgt hieraus kein Freibrief für massenhafte biometrische Indexierung und algorithmische Identifizierung. Die Kategorie der „manifestly public data“ relativiert weder die strikte Erforderlichkeit noch das spezielle unionsrechtliche Verbot des Art. 5 Abs. 1 lit. e KI-VO.⁵⁰

3. Der biometrische Treffer als automatisierte Bewertung: Art. 7 und 11 RL (EU) 2016/680, § 54 BDSG

Eine weitere unionsrechtliche Leitnorm ist Art. 11 RL (EU) 2016/680. Danach sind Entscheidungen, die ausschließlich auf automatisierter Verarbeitung beruhen und für die betroffene Person eine nachteilige Rechtswirkung oder eine ähnlich erhebliche Beeinträchtigung entfalten, grundsätzlich verboten; dies gilt erst recht, wenn sensible Datenkategorien betroffen sind.⁵¹ Art. 26 Abs. 10 KI-VO übernimmt denselben Gedan-

ken ausdrücklich für nachträgliche biometrische Fernidentifizierung.⁵²

Dogmatisch bedeutsam ist zudem Art. 7 RL (EU) 2016/680. Die Richtlinie verlangt, dass personenbezogene Daten, die auf Tatsachen beruhen, von solchen unterschieden werden, die auf persönlichen Einschätzungen beruhen.⁵³ Überträgt man diese Unterscheidung auf biometrische Treffer, spricht viel dafür, den algorithmischen Ähnlichkeitsscore nicht als Tatsache, sondern als technische Bewertung eines Wahrscheinlichkeitsverhältnisses einzuordnen. Selbst wenn man dies nicht strikt kategorisch versteht, folgt jedenfalls, dass der biometrische Treffer dogmatisch nicht als selbsttragender Identitätsbeweis behandelt werden kann. Er ist Ermittlungsansatz, nicht Tatbestandssubstitut.⁵⁴

Diese Erkenntnis hat unmittelbare strafprozessuale Folgen. Ein Treffer darf weder ohne qualifizierte menschliche Verifikation den Tatverdacht tragen noch allein die Grundlage für weitere belastende Maßnahmen bilden. Wo das Gesetz dies nicht ausdrücklich klarstellt, droht ein struktureller Verstoß gegen Art. 11 RL (EU) 2016/680, § 54 BDSG und Art. 26 Abs. 10 KI-VO. Die unionsrechtliche Dogmatik verlangt also nicht nur eine menschliche „Endabnahme“, sondern eine echte inhaltliche Nachprüfung, die den algorithmischen Vorschlag materiell verantwortet.⁵⁵

4. GRCh, EMRK und GG

Die unionsrechtliche Vorprägung erschöpft sich nicht in Sekundärrecht. Nationale Regelungen über biometrische Fernidentifizierung bewegen sich zugleich im Anwendungsbereich der Grundrechtecharta. Maßgeblich sind insbesondere Art. 7 GRCh (Achtung des Privatlebens),⁵⁶ Art. 8 GRCh (Schutz personenbezogener Daten),⁵⁷ Art. 21 GRCh (Diskriminierungsverbot)⁵⁸ und Art. 47 GRCh⁵⁹ (wirksamer Rechtsschutz und faires Verfahren).⁶⁰ Ergänzend sichern Art. 6 und Art. 8 EMRK Verfahrensfairness und Privatheit. Gerade im

⁴⁷ Art. 10 RL (EU) 2016/680; Braun (Fn. 5), BDSG § 48 Rn. 4–7; Schwichtenberg (Fn. 5), BDSG § 48 Rn. 2–7; Frenzel (Fn. 5), BDSG § 48 Rn. 3–4; Teichmann, NJOZ 2026, 705 (707 Rn. 22).

⁴⁸ Frenzel (Fn. 5), BDSG § 48 Rn. 5–9; Thiel, in: Simitis/Hornung/Spiecker gen. Döhmman (Hrsg.), Nomos Kommentar, Datenschutzrecht, 2. Aufl. 2025, BDSG § 48 Rn. 8–21; Kampert, in: Sydow/Marsch (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, Handkommentar, 3. Aufl. 2022, BDSG § 48 Rn. 19–22.

⁴⁹ Vgl. EDPB (Fn. 8), Ziff. 3.1.3.4; FRA (Fn. 8), S. 23.

⁵⁰ Art. 10 lit. c RL (EU) 2016/680; vgl. EuGH, Urt. v. 4.7.2023 – C-252/21, Rn. 89 ff.; EuGH, Urt. v. 21.12.2023 – C-667/21, Rn. 38 ff.

⁵¹ Art. 11 RL (EU) 2016/680; Mundil, in: Wolff/Brink/v. Ungern-Sternberg (Fn. 44), BDSG § 54 Rn. 1–6; Frenzel (Fn. 5), BDSG § 54 Rn. 1–9; Richter, in: Simitis/Hornung/Spiecker gen. Döhmman (Fn. 48), BDSG § 54 Rn. 1–2; Teichmann, NJOZ 2026, 705 (707 Rn. 24).

⁵² Art. 26 Abs. 5, Abs. 10 VO (EU) 2024/1689; Denga (Fn. 19), KI-VO Art. 26 Rn. 103–105.

⁵³ Art. 7 RL (EU) 2016/680.

⁵⁴ Vgl. AG Reutlingen, Beschl. v. 24.4.2025 – 5 Ds 29 Js 1276/25; BGH, Urt. v. 1.2.2017 = NStZ-RR 2017, 183 (184); vgl. auch EDPB (Fn. 8), Ziff. 3.1.2, 5.3.

⁵⁵ Vgl. Buchner (Fn. 37), KI-VO Art. 14 Rn. 33–37; Hilgendorf/Härtlein (Fn. 3), Art. 14 Rn. 2–14; Denga (Fn. 19), KI-VO Art. 26 Rn. 77; Schwichtenberg (Fn. 5), BDSG § 54 Rn. 4–5; Frenzel (Fn. 5), BDSG § 54 Rn. 1–9.

⁵⁶ Kotzur, in: Geiger/Khan/Kotzur/Kirchmair, EUV AEUV, Kommentar, 7. Aufl. 2023, GR-Charta Art. 7 Rn. 1–3.

⁵⁷ Jarass, in: Jarass, Charta der Grundrechte der Europäischen Union, Kommentar, 4. Aufl. 2021, Art. 8 Rn. 2–3.

⁵⁸ Gerlach, in: von der Groeben/Schwarze/Hatje/Terhechte (Hrsg.), Europäisches Unionsrecht, 8. Aufl. 2025, GRCh Art. 21 Rn. 9–11.

⁵⁹ Kubiciel/Großmann, in: Meyer/Hölscheidt (Hrsg.), Charta der Grundrechte der Europäischen Union, 6. Aufl. 2024, Art. 47 Rn. 1.

⁶⁰ Vgl. FRA (Fn. 8), S. 24; EDPB (Fn. 8), Ziff. 3.1.3.4, 3.2.4.1.

Bereich biometrischer Identifikations- und Speicherregime hat der EGMR immer wieder betont, dass anlasslose oder unverhältnismäßige staatliche Erfassung besonders sensibler personenbezogener Daten strengen Rechtfertigungsanforderungen unterliegt.⁶¹ Besondere Aufmerksamkeit verdient in diesem Zusammenhang die Entscheidung des EGMR im Fall Glukhin gegen Russland. Der Gerichtshof hat erstmals zu Gesichtserkennung in der Strafverfolgung ausdrücklich Stellung genommen und auch die nachträgliche Identifizierung als „particularly intrusive“ eingestuft. Er verlangt ein hohes Maß an Rechtfertigung, eine detaillierte Regelung des Anwendungsbereichs und der Anwendung der Maßnahme sowie wirksame Schutzvorkehrungen; eine allgemein gefasste Rechtsgrundlage genügt nicht. Hervorgehoben wird zudem der „chilling effect“ auf Meinungs- und Versammlungsfreiheit, gerade wenn Gesichtserkennung im Versammlungskontext eingesetzt wird.⁶² Daraus folgt für jede künftige deutsche Eingriffsnorm zwingend eine Verschärfung der Bestimmtheitsanforderungen, insbesondere bei der Auswertung von Versammlungs-Bildmaterial. Die Vorgaben der KI-Verordnung sind insoweit als unionsrechtliche Mindestanforderungen, nicht als konventionsrechtliche Höchstgrenze zu lesen.

National bleibt die hessenDATA-Entscheidung des Bundesverfassungsgerichts die Leitentscheidung. Das Gericht hat die automatisierte Datenanalyse als eigenständigen Eingriff qualifiziert, weil sie aus verstreuten Einzelinformationen neues, verdichtetes Wissen erzeugt und damit die Eingriffsqualität gegenüber der bloßen Datenhaltung erheblich steigert.⁶³ Diese Argumentation gilt für biometrische Fernidentifizierung in verschärfter Form. Gesichtserkennung ist nicht nur Datenanalyse, sondern die algorithmische Zuordnung eines unverwechselbaren körperlichen Merkmals zu einer konkreten Person. Sie berührt daher die informationelle Selbstbestimmung besonders intensiv und kann bei systematischem Einsatz erhebliche Einschüchterungseffekte entfalten.⁶⁴

Die unionsrechtliche und die verfassungsrechtliche Perspektive laufen damit nicht auseinander, sondern verstärken einander. Gerade die Kombination aus KI-Verordnung, RL (EU) 2016/680 und hessenDATA zwingt zu einer bereichsspezifischen, hinreichend bestimmten und eng begrenzten Rechtsgrundlage. Eine offene Ermächtigung, deren Konturen erst im Vollzug sichtbar werden, ist weder unions- noch verfassungsrechtlich tragfähig.⁶⁵

⁶¹ EGMR, Urt. v. 4.12.2008 – 30562/04, 30566/04 = NJOZ 2010, 696 (700); EGMR, Urt. v. 13.2.2020 – 45245/15 = NJOZ 2022, 476 (479 f.).

⁶² EGMR, Urt. v. 4.7.2023 – 11519/20, Rn. 83, 86–89; *Hahn* (Fn. 16), S. 205–208; *Palmiotto/González*, Computer Law & Security Review 50 (2023), 105857.

⁶³ BVerfG, Urt. v. 16.2.2023 – 1 BvR 1547/19, 1 BvR 2634/20 = NJW 2023, 1196 (1197 ff.).

⁶⁴ BVerfG, Urt. v. 18.12.2018 – 1 BvR 142/15 = NJW 2019, 827 (828 ff. Rn. 34 ff.); FRA (Fn. 8), S. 27.

⁶⁵ DSK (Fn. 12).

V. Der deutsche Reformdiskurs als Fallstudie europäischen Strafverfahrensrechts

1. Keine tragfähige Rechtsgrundlage im geltenden Strafverfahrensrecht

Nach geltendem Recht fehlt es an einer spezialgesetzlichen strafprozessualen Eingriffsnorm für KI-gestützte biometrische Fernidentifizierung. Ein Rückgriff auf §§ 161, 163 StPO scheitert an der spezifischen Eingriffsqualität der Maßnahme. Wer biometrische Identifizierung aus Bildmaterial automatisiert betreibt, greift nicht lediglich in ein unspezifisches Datenermittlungsfeld ein, sondern nutzt eine Technik, die hochsensible Daten verarbeitet, neue Zuordnungswahrscheinlichkeiten erzeugt und potentiell große Personengruppen betrifft.⁶⁶ Diese Bewertung steht im Einklang mit dem Hauptergebnis der einschlägigen Monographie *Hahns*, die nach umfassender verfassungs-, unions- und strafprozessrechtlicher Prüfung zu dem Befund gelangt, dass derzeit keine taugliche strafprozessuale Rechtsgrundlage für den Einsatz automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger existiert.⁶⁷ Insbesondere § 98c StPO – die in Praxis und Teilen der Literatur herangezogene Vorschrift – erweist sich als ungeeignet. *Hahn* beschreibt die Norm zutreffend als „materiell weitgehend und formell vollständig voraussetzungslos“: Sie verlangt weder eine Katalogtat noch einen gesteigerten Tatverdacht, sieht keine schriftliche oder richterliche Anordnung vor, kennt keine Subsidiaritätsklausel und keine Benachrichtigungspflicht; auch ist sie nicht in den Verfahrensregelungen des § 101 StPO verankert.⁶⁸ Vor allem aber genügt § 98c StPO nicht den Anforderungen der Bestimmtheit und Normenklarheit. Sein Zweck („zur Aufklärung einer Straftat“) ist mit Blick auf die Eingriffsintensität automatisierter Gesichtserkennung zu unbestimmt; das technische Eingriffsinstrument ist nicht spezifiziert; die zum Abgleich zugelassenen Datenbanken sind nicht hinreichend begrenzt; die Verarbeitung höchstpersönlicher biometrischer Merkmale tritt aus der Norm nicht hervor.⁶⁹ Diese Defizite addieren sich nicht nur zu einem einfachgesetzlichen Mangel, sondern führen unmittelbar in den unionsrechtlichen Spezifitätskonflikt mit Art. 8 RL (EU) 2016/680 und Art. 26 Abs. 10 KI-VO.

Nicht überzeugender ist die Konstruktion einer Normenkumulation aus §§ 98a, 98c, 100h oder 163f StPO. Sie zerlegt eine einheitliche technische Gesamtmaßnahme künstlich in Teilschritte, um das Fehlen einer eigens auf biometrische Fernidentifizierung zugeschnittenen Ermächtigung zu kaschieren. Methodisch trägt dies schon deshalb nicht, weil die Verknüpfung von automatisierter Bilderfassung, Merkmalsextraktion, datenbankgestütztem Vergleich und algorithmischer Priorisierung eine neue Eingriffsqualität erzeugt, die keine der Ein-

⁶⁶ *Martini*, NVwZ Extra 1–2/2022, 1 (10 f.); DSK (Fn. 12); *Teichmann*, NStZ 2026, 457 (462).

⁶⁷ *Hahn* (Fn. 16), S. 234, 322 Ziff. 7.

⁶⁸ *Hahn* (Fn. 16), S. 215–218; *Körffler*, Datenschutz-Nachrichten 4 (2014), 146 (148); vgl. *Singelstein*, NStZ 2012, 593 (606).

⁶⁹ *Hahn* (Fn. 16), S. 219 ff., 228.

zelbefugnisse für sich genommen abbildet.⁷⁰ Hinzu kommt, dass auch die regelmäßig hilfsweise herangezogenen §§ 98a, 98b, 81b Abs. 1 Alt. 1, 100h Abs. 1 S. 1 Nr. 1, 163b Abs. 1 S. 1 sowie 161, 163 StPO und § 48 BDSG keine tragfähige Eingriffsgrundlage bilden, weil keine dieser Normen die spezifische Verbindung von Bildverarbeitung, Merkmalsextraktion, datenbankgestütztem biometrischem Abgleich und algorithmischer Priorisierung tatbestandlich erfasst.⁷¹

Dieser Befund lässt sich unionsrechtlich zuspitzen. Art. 8 RL (EU) 2016/680 verlangt eine hinreichend bestimmte gesetzliche Grundlage gerade für Zweck, Datenart und Zielrichtung der Verarbeitung. Die KI-Verordnung knüpft zudem spezifische Anforderungen an genau bezeichnete Systemkategorien. Eine generalisierende oder additiv konstruierte Ermächtigungsgrundlage läuft deshalb nicht nur in das nationale Wesentlichkeitsproblem, sondern zugleich in ein unionsrechtliches Spezifizitätsdefizit.⁷²

2. Der gescheiterte § 98d StPO-E

Der Entwurf eines § 98d StPO sollte den nachträglichen Abgleich von Bild- und Stimmerkmalen mit öffentlich zugänglichen Daten aus dem Internet mittels automatisierter Datenverarbeitung ermöglichen. Positiv hervorzuheben waren der Versuch einer besonderen Eingriffsnorm, das Verbot des Echtzeitabgleichs und die Beschränkung auf schwere Katalogtaten.⁷³ Gleichwohl blieb der Entwurf im unionsrechtlichen entscheidenden Punkt defizitär.

Sein Hauptmangel lag in der Ausblendung der technischen Vorfrage. Der Entwurf tat so, als ließe sich ein biometrischer Abgleich mit „öffentlich zugänglichen Daten aus dem Internet“ normieren, ohne sich zur erforderlichen Datenbankarchitektur zu verhalten. Genau darin liegt aber die unionsrechtliche Scheidelinie, denn soweit die Suchfunktion nur über einen gescrapten Gesichtsindeks realisiert werden kann, stößt sie an Art. 5 Abs. 1 lit. e KI-VO. Ein strafprozessuales Gesetz, das diese Vorfrage offenlässt, ist nicht nur technisch unpräzise, sondern normativ unvollziehbar.⁷⁴

Hinzu trat, dass der Entwurf die aus Art. 10 und 11 RL (EU) 2016/680 sowie § 48 und § 54 BDSG folgenden Sicherungen nur unzureichend verarbeitete. Es fehlten spezifische Regelungen zur manuellen Verifikation, zu Dokumentation und Nachvollziehbarkeit, zu systematischen Fehlerrisiken und zum Diskriminierungsschutz. Ebenso wenig adressierte der Entwurf die für das Strafverfahren zentrale Frage, welche

technischen Angaben zur eingesetzten Software aktenkundig zu machen und der Verteidigung zugänglich zu halten sind.⁷⁵

Der gescheiterte § 98d StPO-E zeigt damit exemplarisch, worin der methodische Fehler des bisherigen Reformdiskurses liegt, da er die KI-Verordnung und die RL (EU) 2016/680 als nachgelagerte Vollzugsprobleme behandelt, obwohl sie den legislativen Ausgangspunkt bilden müssten. Nicht der Vollzug hat zu prüfen, ob eine normierte Befugnis mit Art. 5 Abs. 1 lit. e KI-VO kollidiert; der Gesetzgeber selbst muss den Konflikt auflösen, indem er verbotene Konstellationen gar nicht erst erfasst.⁷⁶

Der Befund gilt der Sache nach fort. Zwar hat die Bundesregierung mit dem Regierungsentwurf vom 29.4.2026 einen zweiten Anlauf für einen § 98d StPO-E unternommen, der den automatisierten Abgleich mit im Internet öffentlich zugänglichen biometrischen Daten bei Straftaten von auch im Einzelfall erheblicher Bedeutung unter Subsidiaritäts-, Protokollierungs- und Benachrichtigungsvorgaben zulassen will. Die Entwurfsbegründung schließt den Aufbau einer dauerhaften behördlichen Gesichtsdatenbank ausdrücklich aus.⁷⁷ Die unionsrechtliche Kernfrage bleibt damit unbeantwortet: Wo die Suchfunktion technisch einen durch ungezieltes Scraping erzeugten – gegebenenfalls beim privaten Anbieter vorgehaltenen – Gesichtsindeks voraussetzt, führt die Verlagerung der Indexbildung auf die Anbieterseite nicht aus Art. 5 Abs. 1 lit. e KI-VO heraus.

3. Der Koalitionsvertrag 2025 und das unionsrechtliche Dilemma des Internetabgleichs

Der Koalitionsvertrag von 2025 belegt, dass der politische Regelungsdruck fortbesteht. Dogmatisch lässt sich die Formel der „retrograden biometrischen Fernidentifizierung“ aber nur auf zwei unterschiedliche Weisen lesen – mit gegensätzlicher Rechtsfolge. Gemeint sein kann erstens die nachträgliche Suche in einem geschlossenen, rechtmäßig erhobenen Referenzbestand. Diese Konstellation ist unionsrechtlich nicht schlechthin ausgeschlossen, verlangt jedoch eine enge spezialgesetzliche Ausgestaltung. Gemeint sein kann zweitens die internetweite biometrische Suche in öffentlich zugänglichen Bildbeständen. Diese Konstellation stößt an das unionsrechtliche Verbot gescraper Gesichtsindeks.⁷⁸

Gerade hierin liegt das Dilemma, denn je attraktiver die Maßnahme kriminalpolitisch erscheint, desto näher rückt sie an die unionsrechtlich verbotene offene Datenbasis. Ein Gesetz, das wirklich wirksam internetweit suchen will, gerät in Konflikt mit Art. 5 Abs. 1 lit. e KI-VO. Ein Gesetz, das nur innerhalb geschlossener, rechtmäßig erhobener Bestände sucht, ist unionsrechtlich eher denkbar, liefert aber gerade nicht die vielbeschworene „Suche im Internet“. Die politi-

⁷⁰ Martini, NVwZ Extra 1–2/2022, 1 (10 f.); Singelstein, NSStZ 2012, 593 (595 ff.).

⁷¹ Hahn (Fn. 16), S. 230 ff.; Gerhold, in: Graf (Hrsg.), Beck'scher Online-Kommentar, Strafprozessordnung, Stand: 1.7.2026, § 98c Rn. 1.

⁷² Art. 8 RL (EU) 2016/680; Art. 6 Abs. 2 VO (EU) 2024/1689; Klawonn (Fn. 36), KI-VO Art. 6 Rn. 16–18; Denga (Fn. 19), KI-VO Art. 26 Rn. 77; Teichmann, NSStZ 2026, 457 (459).

⁷³ BT-Drs. 20/12806, S. 14–15.

⁷⁴ Lewandowski (Fn. 7); Deutscher Bundestag (Fn. 7), S. 6 f.

⁷⁵ Vgl. DSK (Fn. 12); Rückert, StV 2025, 350.

⁷⁶ Lewandowski (Fn. 7).

⁷⁷ Regierungsentwurf eines Gesetzes zur Änderung der Strafprozessordnung – digitale Ermittlungsmaßnahmen v. 29.4.2026, S. 15 (zuvor Referentenentwurf des BMJV v. 12.3.2026, S. 13).

⁷⁸ Bundesregierung (Fn. 1); Deutscher Bundestag (Fn. 7), S. 6 f.

sche Redeweise verdeckt diese Alternative, die dogmatische Analyse muss sie offenlegen.

Damit wird der deutsche Reformdiskurs zu einer instruktiven Fallstudie europäischen Strafverfahrensrechts. Europäisierung bedeutet hier nicht Vollvereinheitlichung, sondern die Errichtung eines normativen Korridors, und zwar nationale Gestaltung innerhalb unionsrechtlich gezogener Grenzen. Der deutsche Gesetzgeber kann sich innerhalb dieses Korridors bewegen, nicht aber aus ihm ausbrechen.

VI. Beweisverwertung und Verteidigung

1. Der Beschluss des AG Reutlingen

Besondere Aufmerksamkeit verdient der Beschluss des AG Reutlingen vom 24.4.2025. Das Gericht ordnete wegen der Schwierigkeit der Sach- und Rechtslage die Beordnung eines Pflichtverteidigers an, weil der Tatverdacht maßgeblich auf einer video- und softwaregestützten Gesichtserkennung beruhte, während nähere Angaben zu Algorithmus, Referenzdaten und Qualitätskriterien fehlten.⁷⁹ Das Gericht hob hervor, dass die Verwertbarkeit des Treffers und sein Beweiswert ungeklärt seien; ein bloßes Etikett als „Ermittlungsunterstützung“ genüge nicht, wenn auf dem Treffer faktisch der Tatverdacht ruhe.⁸⁰

Die Bedeutung der Entscheidung liegt nicht darin, dass sie bereits eine ausdifferenzierte Dogmatik der KI-Beweisführung entwickelt hätte. Ihr Wert liegt vielmehr in der prozessualen Sensibilisierung. Das Gericht erkennt, dass technische Intransparenz nicht nur ein Problem materieller Richtigkeit, sondern ein Strukturproblem des fairen Verfahrens ist. Wo Anklage und gerichtliche Überzeugungsbildung wesentlich auf einem algorithmischen Prozess beruhen, dessen Funktionsbedingungen nicht offenliegen, ist wirksame Verteidigung gefährdet.⁸¹

2. Der biometrische Treffer als Ermittlungsansatz, nicht als selbsttragender Beweis

Aus dogmatischer Sicht liegt es nahe, den biometrischen Treffer zunächst nur als Ermittlungsansatz zu behandeln. Dies entspricht sowohl Art. 11 RL (EU) 2016/680 und Art. 26 Abs. 10 KI-VO als auch dem deutschen Grundsatz freier,

aber rational kontrollierter Beweiswürdigung. Ein Systemoutput, dessen Zustandekommen das Gericht nicht nachvollziehen kann, eignet sich nicht als selbsttragende Basis richterlicher Überzeugungsbildung.⁸²

Daraus folgt allerdings nicht notwendig ein ausnahmsloses Beweisverwertungsverbot. Die deutsche Dogmatik kennt bekanntlich keine generelle fruit-of-the-poisonous-tree-Lehre. Sie arbeitet mit Abwägungen, die auf Schutzzweck, Gewicht des Verstoßes und Bedeutung der betroffenen Verfahrensgarantien abstellen.⁸³ Gerade deshalb ist im Bereich biometrischer Fernidentifizierung zwischen Verwertbarkeit und Beweisgewicht zu differenzieren. Ein rechtswidrig gewonnener oder methodisch intransparenter Treffer kann entweder unverwertbar sein oder – was praktisch nicht minder relevant ist – evidenziell so geschwächt werden, dass er einen Tatverdacht oder gar eine Verurteilung nicht tragen kann. Die strafprozessuale Behandlung biometrischer Treffer muss zudem dem empirisch belegten „automation bias“ Rechnung tragen, also der menschlichen Tendenz, automatisierten Vorschlägen unkritisch zu folgen. Die in den USA dokumentierten Fälle der Festnahme Unbeteiligter nach Gesichtserkennung-Treffern – Williams, Oliver, Parks, Sawyer, Reid, Woodruff – lassen sich nach eingehender Aufarbeitung gerade nicht allein auf technisches Versagen zurückführen, sondern beruhen wesentlich auf menschlichen Folgefehlern wie ungeprüft übernommene Treffer, vorschnelle Wahllichtbildvorlagen oder mangelnde Schulung der ermittelnden Beamten.⁸⁴ Diese Erfahrung muss in der deutschen Dogmatik nicht erst nachvollzogen werden; sie zwingt vielmehr bereits jetzt dazu, an den biometrischen Treffer einen verschärften Maßstab anzulegen und ihn ohne nachweisbar qualifizierte, dokumentierte und unabhängige menschliche Verifikation strafprozessual nicht durchschlagen zu lassen.

Für beides spricht viel, wenn zwei Bedingungen kumulieren: erstens das Fehlen einer tragfähigen Rechtsgrundlage oder der Rückgriff auf unionsrechtlich gesperrte Datengrundlagen, zweitens die fehlende Nachvollziehbarkeit des konkreten Systemeinsatzes. Wer nicht offenlegen kann, mit welcher Softwareversion, welchem Schwellwert, welchem Referenzbestand und welchen Qualitätsparametern gearbeitet wurde, verschiebt das Risiko technischer Unsicherheit einseitig auf den Beschuldigten. Das ist mit einem rechtsstaatlichen Strafverfahren kaum vereinbar.⁸⁵

⁷⁹ AG Reutlingen, Beschl. v. 24.4.2025 – 5 Ds 29 Js 1276/25; *Kämpfer/Travers*, in: Kudlich (Hrsg.), Münchener Kommentar zur Strafprozessordnung, Bd. 1, 2. Aufl. 2023, § 140 Rn. 35–36; *Krawczyk*, in: Graf (Fn. 71), § 140 Rn. 27, 31–35; BRAK, Gesichtserkennungssoftware im Strafprozess – nur mit Anwalt v. 11.12.2025, abrufbar unter <https://www.brak.de/newsroom/news/gesichtserkennungssoftware-im-strafprozess-nur-mit-anwalt/> (22.6.2026); *Rückert*, StV 2025, 350.

⁸⁰ AG Reutlingen, Beschl. v. 24.4.2025 – 5 Ds 29 Js 1276/25; OLG Stuttgart, Beschl. v. 8.5.2001 – 3 Ss 13/2001 = NStZ 2001, 603.

⁸¹ Vgl. *Murmann*, in: Rotsch/Saliger/Tsambikakis (Hrsg.), Nomos Kommentar, StPO, Bd. 1, 2025, § 261 Rn. 87–91; *Bartel*, in: Schneider (Hrsg.), Münchener Kommentar zur Strafprozessordnung, Bd. 2, 2. Aufl. 2024, § 261 Rn. 5–8, 139.

⁸² Art. 11 RL (EU) 2016/680; Art. 26 Abs. 5, Abs. 10 VO (EU) 2024/1689; *Murmann* (Fn. 81), § 261 Rn. 217–218; *Bartel* (Fn. 81), § 261 Rn. 5, 67–70; *Tiemann*, in: Barthe/Gericke (Hrsg.), Karlsruher Kommentar zur Strafprozessordnung, 9. Aufl. 2023, § 261 Rn. 5–10.

⁸³ BGH, Urt. v. 7.3.2006 – 1 StR 316/05 Rn. 12, 24–26; *Bartel* (Fn. 81), § 261 Rn. 139, 143; *Bock*, in: Rotsch/Saliger/Tsambikakis (Fn. 81), § 244 Rn. 318–321; *Murmann* (Fn. 81), § 261 Rn. 62.

⁸⁴ *Hahn* (Fn. 16), S. 250 ff., 262 ff., 273 ff.; vgl. *Albright/Garrett*, Boston University Law Review 102 (2022), 511.

⁸⁵ Vgl. AG Reutlingen, Beschl. v. 24.4.2025 – 5 Ds 29 Js 1276/25; *Momsen*, in: Chibanguza/Kuß/Steege (Hrsg.), Künstliche Intelligenz, 2. Aufl. 2025, G. Rn. 49–54; *Hilgendorf*/

3. Verteidigungsrechte im technisch intransparenten Verfahren

Die eigentliche verfahrensdogmatische Herausforderung liegt in den Verteidigungsrechten. Art. 47 GRCh, Art. 6 EMRK und das aus Art. 20 Abs. 3 GG folgende Gebot fairer Verfahrensgestaltung verlangen, dass der Beschuldigte die ihn belastende Identifizierung wirksam angreifen kann.⁸⁶ Dies setzt jedenfalls voraus, dass wesentliche technische Informationen aktenkundig werden wie Systembezeichnung und -version, Herkunft und rechtliche Qualität des Referenzbestands, Eingabe- und Ausgabeparameter, Dokumentation der menschlichen Nachprüfung, bekannte Fehlerraten und etwaige Bias-Tests.⁸⁷

Die Einwendung, Herstellergeheimnisse stünden einer weitergehenden Offenlegung entgegen, greift im Strafverfahren nur eingeschränkt. Wo der Staat eine bestimmte Technologie als tragendes Mittel der Identifizierung einsetzt, trägt er auch die Verantwortung für deren justizielle Prüfbarkeit. Schutzwürdige Geheimhaltungsinteressen können besondere Sicherungsmechanismen rechtfertigen; sie dürfen aber nicht dazu führen, dass die Verteidigung gerade den belastungs-tragenden technischen Kern nicht angreifen kann. Im Zweifel muss der Staat das Risiko fehlender Transparenz tragen, nicht der Beschuldigte.⁸⁸

Damit verschiebt sich auch die Perspektive auf die Gesetzgebung. Eine zukünftige Eingriffsnorm darf sich nicht in materiellen Einsatzvoraussetzungen erschöpfen. Sie muss auch verteidigungsfunktionale Transparenznormen enthalten. Sonst bleibt die Maßnahme zwar vielleicht verwaltungsrechtlich kontrollierbar, strafprozessual aber defizitär. Das europäische Strafverfahrensrecht verlangt hier nicht weniger, sondern mehr Normklarheit.

VII. Eckpunkte einer unions- und verfassungskonformen Neuregelung

1. Regelungsfähige und regelungsunfähige Konstellationen

Aus dem Vorstehenden folgt zunächst eine negative Leitentscheidung. Ein Gesetz, das die automatisierte biometrische Suche in offen zugänglichen Internetbildern oder in auf ungezieltem Scraping beruhenden Gesichtsindizes zulassen will, ist unionsrechtlich nicht tragfähig. Eine solche Konstellation ist nicht nur regelungsbedürftig, sondern regelungs-unfähig.⁸⁹

Roth-Isigkeit, Die neue Verordnung der EU zur Künstlichen Intelligenz, 2. Aufl. 2025, § 6 Rn. 3; *Buchner/Petri*, in: *Kühling/Buchner* (Fn. 5), DS-GVO Art. 6 Rn. 172e; *Martini/Kemper*, CR 2023, 341; *Rückert*, StV 2025, 350.

⁸⁶ BVerfG, Urt. v. 16.2.2023 – 1 BvR 1547/19, 1 BvR 2634/20 = NJW 2023, 1196 (1199).

⁸⁷ *Schwichtenberg* (Fn. 5), BDSG § 48 Rn. 5–6; *Frenzel* (Fn. 5), BDSG § 48 Rn. 5–9; *Thiel* (Fn. 48), BDSG § 48 Rn. 8–21; AG Reutlingen, Beschl. v. 24.4.2025 – 5 Ds 29 Js 1276/25.

⁸⁸ Vgl. *Rückert*, StV 2025, 350; *Martini/Kemper*, CR 2023, 341.

⁸⁹ Art. 5 Abs. 1 lit. e VO (EU) 2024/1689; *Hilgendorf/Härtlein* (Fn. 3), Art. 5 Rn. 45–48.

Regelungsfähig bleiben demgegenüber nur eng begrenzte Formen der nachträglichen biometrischen Suche: erstens der Abgleich mit geschlossenen, rechtmäßig erhobenen polizeilichen Referenzdatenbeständen; zweitens eine fallbezogene Nachsuche in rechtmäßig gesichertem Videomaterial, das räumlich, zeitlich und sachlich begrenzt ist.⁹⁰ Beide Konstellationen bedürfen jedoch einer spezifischen normativen Einhegung. Weder der Bestand „rechtmäßig erhoben“ noch die Verwendung der Formulierung „geschlossener Datensatz“ dürfen der Verwaltung zur freien Ausfüllung überlassen bleiben.

2. Mindestinhalt einer spezialgesetzlichen Eingriffsnorm

Eine unions- und verfassungskonforme Neuregelung sollte mindestens sieben Elemente enthalten.

Erstens bedarf es einer präzisen Bestimmung der zulässigen Datengrundlagen. Die Norm muss positiv definieren, welche Referenzbestände verwendet werden dürfen, und negativ klarstellen, dass jede Nutzung von durch ungezieltes Auslesen des Internets oder von Videoüberwachungsanlagen erzeugten Gesichtsindizes ausgeschlossen ist.⁹¹

Zweitens ist eine qualifizierte Eingriffsschwelle erforderlich. Der Einsatz sollte auf besonders schwere Straftaten beschränkt werden und voraussetzen, dass konkrete Tatsachen sowohl für die Begehung einer Katalogtat als auch für den Bezug der gesuchten Person zum Ausgangsbild sprechen. Eine biometrische Suche „ins Blaue hinein“ wäre weder mit Art. 26 Abs. 10 KI-VO noch mit hessenDATA vereinbar.⁹²

Drittens braucht es eine echte Subsidiaritätsklausel. Die Maßnahme darf nur zulässig sein, wenn andere Ermittlungsmaßnahmen wesentlich weniger Erfolg versprechen oder unverhältnismäßig aufwendiger wären.⁹³

Viertens ist ein Richtervorbehalt als Regelfall unverzichtbar; Eilkompetenzen der Staatsanwaltschaft dürfen nur eng begrenzt und an eine kurzfristige richterliche Bestätigung geknüpft werden. Art. 26 Abs. 10 KI-VO gibt hierfür mit dem 48-Stunden-Modell bereits einen unionsrechtlichen Referenzrahmen vor.⁹⁴

Fünftens muss die Norm die qualifizierte menschliche Verifikation ausdrücklich anordnen. Ergebnisse dürfen weder als Beweismittel noch als Grundlage weiterer belastender Maßnahmen verwendet werden, solange sie nicht von einer fachkundigen Person überprüft und dokumentiert wurden. Diese Anforderung folgt nicht nur aus dem Fair-Trial-Gedan-

⁹⁰ ErwG 95, Art. 26 Abs. 10 VO (EU) 2024/1689; *Denga* (Fn. 19), KI-VO Art. 26 Rn. 78–85.

⁹¹ Art. 5 Abs. 1 lit. e, ErwG 43 VO (EU) 2024/1689; *Hilgendorf/Härtlein* (Fn. 3), Art. 5 Rn. 45–48.

⁹² Art. 26 Abs. 10 VO (EU) 2024/1689; *Denga* (Fn. 19), KI-VO Art. 26 Rn. 88–90; BVerfG, Urt. v. 16.2.2023 – 1 BvR 1547/19, 1 BvR 2634/20 = NJW 2023, 1196 (1199 Rn. 52, 1202 ff. Rn. 71 ff.).

⁹³ *Denga* (Fn. 19), KI-VO Art. 26 Rn. 90.

⁹⁴ Art. 26 Abs. 1–3, Abs. 10 VO (EU) 2024/1689; *Denga* (Fn. 19), KI-VO Art. 26 Rn. 88.

ken, sondern unmittelbar aus Art. 11 RL (EU) 2016/680, § 54 BDSG und Art. 26 Abs. 10 KI-VO.⁹⁵

Sechstens bedarf es technischer und prozessualer Transparenzpflichten wie Protokollierung jedes Einsatzes, Dokumentation von Softwareversion, Parametern, Referenzbestand und Verifikationsschritten, regelmäßige Tests auf Genauigkeit und diskriminierende Fehlerraten, Benachrichtigungspflichten und parlamentarische Berichtspflichten.⁹⁶

Siebtens müssen verteidigungsrelevante Offenlegungsrechte normiert werden. Eine Strafprozessordnung, die biometrische Fernidentifizierung zulässt, ohne den Zugang der Verteidigung zu den belastungswesentlichen technischen Informationen sicherzustellen, bleibt unvollständig. Das ist kein Annexproblem, sondern integraler Bestandteil einer rechtsstaatlichen Eingriffsermächtigung.⁹⁷

3. Formulierungsvorschlag

Vor diesem Hintergrund könnte eine Neuregelung in der StPO – in bewusstem Gegenentwurf zum Regierungsentwurf v. 29.4.2026 (oben V. 2.) – in konzentrierter Form wie folgt aussehen:

§ 98d StPO-E – Nachträgliche biometrische Fernidentifizierung

(1) Zur Aufklärung einer in § 100b Abs. 2 bezeichneten besonders schweren Straftat darf das Gericht die nachträgliche biometrische Fernidentifizierung einer Person anordnen, wenn bestimmte Tatsachen den Verdacht einer solchen Tat begründen, das zu vergleichende Bildmaterial einen Bezug zur Tat aufweist und andere Ermittlungsmaßnahmen wesentlich weniger Erfolg versprechen oder aussichtslos wären.

(2) Die Maßnahme ist nur zulässig durch den automatisierten Abgleich mit einem geschlossenen, rechtmäßig erhobenen Referenzdatenbestand polizeilicher Informationssysteme oder mit einem räumlich, zeitlich und sachlich abgegrenzten Bestand rechtmäßig gesicherten Videomaterials.

(3) Unzulässig ist jeder Abgleich mit Datenbanken, die durch ungezieltes Auslesen von Gesichtsbildern aus dem Internet oder von Videoüberwachungsanlagen erstellt oder erweitert wurden.

(4) Bei Gefahr im Verzug kann die Staatsanwaltschaft die Maßnahme vorläufig anordnen; die richterliche Bestätigung ist binnen 48 Stunden einzuholen.

(5) Ergebnisse des automatisierten Abgleichs dürfen nur nach fachkundiger menschlicher Verifikation und deren Dokumentation verwendet werden; eine nachteilige Entscheidung darf nicht ausschließlich auf der Ausgabe des Systems beruhen.

⁹⁵ Art. 11 RL (EU) 2016/680; Art. 26 Abs. 5 und 10 VO (EU) 2024/1689; *Denga* (Fn. 19), KI-VO Art. 26 Rn. 103–105.

⁹⁶ Art. 9–14 VO (EU) 2024/1689; *FRA* (Fn. 8), S. 33–34; *Rückert*, StV 2025, 350.

⁹⁷ AG Reutlingen, Beschl. v. 24.4.2025 – 5 Ds 29 Js 1276/25; *Gaede*, in: Kudlich (Hrsg.), Münchener Kommentar zur Strafprozessordnung, Bd. 4, 2. Aufl. 2025, EMRK Art. 6 Rn. 129–131.

(6) Die Akte muss jedenfalls Angaben zur eingesetzten Software, zur Version, zu den wesentlichen Parametern, zur Herkunft des Referenzbestands, zu den Verifikationsschritten sowie zu den Ergebnissen regelmäßiger Qualitäts- und Bias-Prüfungen enthalten. Der Verteidigung ist Zugang zu diesen belastungswesentlichen Angaben zu gewähren, soweit nicht überwiegende Geheimhaltungsgründe im Einzelfall besondere Sicherungen erfordern.

(7) Betroffene sind nachträglich zu benachrichtigen, sobald dies den Untersuchungszweck nicht gefährdet. Der Einsatz der Vorschrift ist jährlich in anonymisierter Form zu dokumentieren und dem Bundestag zu berichten.

Ferner bedarf es einer eigenständigen Versammlungsklausel. Wird Bildmaterial ausgewertet, das im Zusammenhang mit einer Versammlung gefertigt wurde, muss der Einsatz biometrischer Fernidentifizierung auf Straftaten von – auch im Einzelfall – erheblicher Bedeutung beschränkt werden. Andernfalls droht ein konventions- und unionsrechtlich relevanter Einschüchterungseffekt auf die Versammlungs- und Meinungsfreiheit, den der EGMR im Fall *Glukhin* ausdrücklich problematisiert hat.⁹⁸

Hahn hat einen eigenen, konzentrierten Formulierungsvorschlag in Gestalt eines § 163h StPO vorgelegt, der die Maßnahme dogmatisch im Bereich der Eingriffe der Polizei (§§ 161 ff. StPO) verortet, eine geschlossene Datenbankarchitektur voraussetzt, qualifizierte Lichtbildsachverständige und einen unabhängigen Vier-Augen-Vergleich verlangt, einen Richtervorbehalt mit Eilkompetenz der Staatsanwaltschaft vorsieht und eine Zertifizierungspflicht der eingesetzten Systeme aus Anhang III KI-VO ableitet.⁹⁹ *Hahn* legt den Akzent auf die kriminologisch dokumentierte Fehleranfälligkeit und die innerorganisatorische Qualitätskontrolle. Der hier vorgeschlagene Entwurf akzentuiert demgegenüber die unionsrechtliche Korridor-Funktion und die strafverfahrensrechtliche Verteidigungsdimension. Beide Stoßrichtungen sind miteinander vereinbar. Eine künftige gesetzgeberische Lösung wird beide aufnehmen müssen.

Der Entwurf ist bewusst zweistufig angelegt. Abs. 2 definiert den einzig regelungsfähigen positiven Anwendungsbereich; Abs. 3 zieht die unionsrechtlich gebotene rote Linie. Gerade dieses Zusammenspiel fehlt den bisherigen deutschen Vorhaben. Ohne den negativen Halbsatz gegen gescrapte Gesichtssindizes würde die Norm in unionsrechtlich verbotene Konstellationen hineinlaufen; ohne den positiven Halbsatz zu geschlossenen, rechtmäßig erhobenen Beständen bliebe ihr Anwendungsbereich unbestimmt.¹⁰⁰

Der Vorschlag ist bewusst restriktiv. Er versteht die KI-VO nicht als Lizenz, sondern als Limit. Das ist kriminalpolitisch möglicherweise enttäuschender als die Rede von der „Suche im Internet“. Rechtsstaatlich und unionsrechtlich ist gerade diese Enttäuschung jedoch der Preis normativer Ehrlichkeit.

⁹⁸ EGMR, Urt. v. 4.7.2023 – 11519/20, Rn. 88; *Hahn* (Fn. 16), S. 142 ff., 311 f., 322.

⁹⁹ *Hahn* (Fn. 16), S. 314.

¹⁰⁰ *Lewandowski* (Fn. 7).

VIII. Schluss

Die Debatte über retrograde biometrische Fernidentifizierung ist ein Lehrstück dafür, wie europäisches Strafverfahrensrecht heute entsteht, und zwar nicht als einheitliche europäische Strafprozessordnung, sondern als Verdichtung unionsrechtlicher Verbote, Datenschutzstandards und Grundrechtsgarantien, innerhalb deren der nationale Gesetzgeber nur noch begrenzt frei gestaltet. Die KI-Verordnung zieht mit Art. 5 Abs. 1 lit. e und h absolute oder nahezu absolute Sperren ein; die RL (EU) 2016/680 fordert Gesetzlichkeit, strikte Erforderlichkeit und das Verbot ausschließlich automatisierter belastender Entscheidungen; GG, GRCh und EMRK verlangen eine bereichsspezifische, verhältnismäßige und verteidigungszugängliche Ausgestaltung.

Für den deutschen Reformdiskurs folgt daraus eine klare Unterscheidung. Nachträgliche biometrische Suche in geschlossenen, rechtmäßig erhobenen Beständen kann, unter engen Voraussetzungen, regelbar sein. Die internetweite biometrische Suche in gescrapten Bildbeständen ist es nicht. Wer beides unter dem Begriff der „retrograden Fernidentifizierung“ zusammenzieht, verwischt die unionsrechtlich entscheidende Linie.

Gerade darin liegt die europäische Pointe. Die Frage lautet nicht mehr nur, ob Gesichtserkennung im Strafverfahren nützlich ist. Sie lautet, welche Formen biometrischer Identifizierung das europäische Recht überhaupt noch als rechtsstaatlich verantwortbare Strafverfolgung akzeptiert. Die Antwort ist wesentlich restriktiver, als es der deutsche politische Diskurs bislang erkennen lässt.