Kapitel II. Rechtlicher Rahmen

In diesem Kapitel wird der rechtliche Rahmen des Einsatzes automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger untersucht. Dabei stellt sich im ersten Schritt die Frage, welche rechtlichen Anforderungen an eine Rechtsgrundlage zu stellen sind. Hierfür wird zunächst vertieft herausgearbeitet, welche Vorgaben das deutsche Verfassungsrecht macht (A.).[299] Zudem wird untersucht, ob sich aus dem europäischen Recht darüber hinausgehende konkrete Vorgaben ergeben (B.). In einem zweiten Schritt gilt es dann zu prüfen, ob das geltende Strafprozessrecht eine Rechtsgrundlage bereithält, die diese Voraussetzungen erfüllt (C.).

A. Verfassungsrecht: Anforderungen an die Rechtsgrundlage

Im Zentrum der verfassungsrechtlichen Betrachtung steht das Grundrecht auf informationelle Selbstbestimmung; auch wird kurz auf die Versammlungsfreiheit, den allgemeinen Gleichheitssatz und die Menschenwürde eingegangen. Da das Anliegen dieser Arbeit ist, einen ersten Vorschlag für eine Regulierung von Gesichtserkennung zu erarbeiten, bildet die Rechtsprechung des Bundesverfassungsgerichts den Ausgangspunkt. Sie wird zugrunde gelegt und hiervon ausgehend herausgearbeitet, wie sie auf die Gesichtserkennung zu übertragen ist.

299 Ungeachtet der Normenhierarchie wird das europäische Recht erst anschließend betrachtet, da das deutsche Verfassungsrecht in seiner Auslegung durch das Bundesverfassungsgericht mit dem Recht auf informationelle Selbstbestimmung zu Fragen der (automatisierten) Datenverarbeitung ausdifferenziertere Vorgaben macht. Die für polizeiliche Datenverarbeitung ebenfalls einschlägige JI-Richtlinie (hierzu näher unter B. I. 2.) enthält keine zwingenden Vorgaben des Unionsrechts, sodass das Bundesverfassungsgericht die Zulässigkeit des Einsatzes automatisierter Gesichtserkennung weiterhin am Maßstab des Grundgesetzes überprüfen würde, vgl. nur BVerfGE 155, 119, 163 ff.

I. Recht auf informationelle Selbstbestimmung

"It's not just a difference in degree; it's a difference in kind."
– Bruce Schneier[300]

Das vom Bundesverfassungsgericht erstmals im Volkszählungsurteil 1983 entwickelte Recht auf informationelle Selbstbestimmung[301] dient dazu, die Autonomie des Einzelnen zu sichern, indem es gewährleistet, dass dieser grundsätzlich selbst über die Erhebung und Verwendung seiner Daten bestimmen kann.[302] Es ist kein „Digital-Grundrecht", sondern gilt auch für analoge Datenverarbeitungen. Sein Schutzbereich trägt aber den „modernen Bedingungen der Datenverarbeitung" besonders Rechnung.[303] Diese erlauben nicht nur die Verarbeitung einer Menge an Daten, die auf konventionellem Wege gar nicht bewältigt werden könnte, sondern ermöglichen es auch, Informationen unbegrenzt zu speichern, jederzeit ohne Rücksicht auf Entfernungen in Sekundenschnelle abzurufen und durch Verknüpfung von Daten Rückschlüsse über Personen zu ziehen.[304] Vor diesem Hintergrund ist auch die automatisierte Gesichtserkennung zu betrachten: Der automatisierte sekundenschnelle Abgleich von Millionen Lichtbildern bedeutet nicht nur eine andere *Quantität* als der manuelle Abgleich durch einen Polizeibeamten, sondern auch eine neue *Qualität* der Datenverarbeitung.[305]

1. Schutzbereich

Das Grundrecht auf informationelle Selbstbestimmung schützt die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.[306] Es stellt eine Ausprägung des

300 *Schneier*, The Coming AI Hackers, 2021, 1, https://perma.cc/3B3C-X5CZ.
301 BVerfGE 65, 1.
302 *Eifert*, in: Herdegen/Masing/Poscher/Gärditz, Handbuch des Verfassungsrechts, 2021, § 18 Persönliche Freiheit, Rn. 129.
303 Siehe auch *Kube*, in: Isensee/Kirchhof, Handbuch des Staatsrechts, Band VII, 3. Aufl. 2009, § 148 Rn. 68 („Die Bedeutung der informationellen Selbstbestimmung zu betonen, ist heute – fast 30 Jahre nach dem Volkszählungsurteil – wegen der mittlerweile erreichten Leistungsfähigkeit der elektronischen Datenverarbeitungssysteme […] gebotener denn je.").
304 BVerfGE 65, 1 (42). Vgl. auch BVerfGE 113, 29 (46); 115, 166 (188); 115, 320 (341 f.); 118, 168 (184); 120, 378 (397); 130, 151 (183).
305 So auch *Martini*, NVwZ-Extra 1-2/2022, 1, 7.
306 BVerfGE 65, 1 (43).

allgemeinen Persönlichkeitsrechts gem. Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG dar.[307] Von diesem unterscheidet es sich in seiner Loslösung des Denkens in unterschiedlichen „Sphären": Das Recht auf informationelle Selbstbestimmung schützt alle personenbezogenen Daten,[308] unabhängig davon, ob sie der Sozial-, Privat- oder Intimsphäre zuzuordnen sind.[309] Unter den Bedingungen der automatischen Datenverarbeitung gibt es kein „belangloses" Datum mehr,[310] da neue Technologien es ermöglichen, große Mengen von Daten miteinander zu verknüpfen und daraus weitere Rückschlüsse zu ziehen. Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare Person beziehen.[311] Identifizierbar ist eine Person dann, wenn mithilfe weiterer Informationen ihre Identität

307 Siehe nur BVerfGE 118, 168 (184); 115, 166 (187); *Eifert*, in: Herdegen/Masing/Poscher/Gärditz, Handbuch des Verfassungsrechts, 2021, § 18 Persönliche Freiheit, Rn. 91. Vgl. auch *Kube*, in: Isensee/Kirchhof, Handbuch des Staatsrechts, Band VII, 3. Aufl. 2009, § 148 Rn. 66 („eigenständige Ausformung"); Dreier GG/*Barczak*, 4. Aufl. 2023, GG Art. 2 Abs. 1 Rn. 91 („bereichsspezifische Konkretisierung" des allgemeinen Persönlichkeitsrechts); *Schwabenbauer*, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, Kapitel G. Informationsverarbeitung im Polizei- und Strafverfahrensrecht, Rn. 88 („Facette" des allgemeinen Persönlichkeitsrechts).

308 BVerfGE 65, 1 (42); 118, 168 (184). Das Bundesverfassungsgericht verwendet wechselnd (teilweise innerhalb einer Entscheidung) die Begriffe „personenbezogene Daten", „persönliche Daten" (so auch in BVerfGE 65, 1 (43)) und „personenbezogene Informationen" (siehe z. B. BVerfGE 115, 166 (190)). Vgl. auch BVerfGE 67, 100 (143) („auf sie [die Grundrechtsträger] bezogene[…], individualisierte[…] oder individualisierbare[…] Daten").

309 Dreier GG/*Barczak*, 4. Aufl. 2023, GG Art. 2 Abs. 1 Rn. 92; vgl. auch BVerfGE 150, 244 (264).

310 So bereits BVerfGE 65, 1 (45); siehe auch BVerfGE 115, 320 (350); 118, 168 (185); 120, 378 (399).

311 Zur Definition wird § 46 Nr. 1 BDSG (oder der wortgleiche Art. 4 Nr. 1 DSGVO) herangezogen, BVerfG (K), NJW 2018, 2395, 2396; v. Münch/Kunig/*Kunig/Kämmerer*, 7. Aufl. 2021, GG Art. 2 Rn. 76; Dreier GG/*Barczak*, 4. Aufl. 2023, GG Art. 2 Abs. 1 Rn. 92. Danach sind personenbezogene Daten „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser Person sind, identifiziert werden kann". Vgl. hingegen noch BVerfGE 65, 1 (42): „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person (personenbezogene Daten [vgl. § 2 Abs. 1 BDSG])".

ermittelt werden kann;[312] maßgeblich sind dabei die Möglichkeiten der verarbeitenden Stelle,[313] im Fall der Gesichtserkennung also die der Strafverfolgungsbehörden.

Entscheidend ist daher zunächst die Frage, ob beim Einsatz von Gesichtserkennung zur Identitätsermittlung personenbezogene Daten verarbeitet werden. Das trifft zunächst ohne Weiteres auf die verwendeten Bilder zu, denn Lichtbilder enthalten personenbezogene Daten, wenn die abgebildete Person erkennbar ist.[314] Das ist bei den zur Gesichtserkennung verwendeten Bildern der Fall, sowohl bei den Bildern in der Datenbank (meist Porträtfotos) als auch bei den Aufnahmen, auf denen der zu identifizierende Verdächtige abgebildet ist.[315]

Auch die Embeddings als numerische Darstellungen der Gesichter[316] sind personenbezogene Daten. Der Umstand, dass sich aus dem Embedding selbst die Identität oder der Name der Person nicht direkt ergeben, steht dem nicht entgegen. Das Bundesverfassungsgericht hat bereits mit Blick auf automatisierte Kfz-Kennzeichenkontrollen festgestellt, dass es für die Feststellung eines Personenbezugs unschädlich sei, dass die Autokennzeichen selbst den Namen des Fahrzeughalters nicht anzeigen.[317] Maßgeblich sei insofern allein, dass sich das Kennzeichen eindeutig einer bestimmten Person zuordnen lässt und damit personenbezogene Informationen vermitteln kann.[318] Das trifft auf die für die Gesichtserkennung erstellten Embeddings ebenfalls zu.[319] Diese sind in der Datenbank mit den weiteren Informationen zu einer Person (insbesondere Lichtbild, Name, Adresse)

312 Vgl. nur Paal/Pauly/*Ernst*, 3. Aufl. 2021, DS-GVO Art. 4 Rn. 8; BeckOK DatenschutzR/*Schild*, 46. Ed., Stand: 1.11.2023, BDSG § 46 Rn. 2.

313 EuGH, NJW 2016, 3579, 3581 (Personenbezug, wenn die verarbeitende Stelle „über rechtliche Mittel verfügt, die es […] erlauben, die betreffende Person anhand der Zusatzinformationen […] bestimmen zu lassen").

314 Deutlich BVerwG, NJW 2019, 2556 (2561). Auch das Bundesverfassungsgericht geht davon aus, dass durch Videoaufnahmen personenbezogene Daten verarbeitet werden, siehe nur BVerfG, NVwZ 2007, 688, 690 und BVerfGE 120, 378 (399 ff.).

315 Zu verneinen wäre der Personenbezug nur, wenn die Qualität der Aufnahmen so schlecht ist, dass eine Identifizierung unter keinen Umständen möglich wäre; solche Aufnahmen würden dann aber erst gar nicht zur Identifizierung mit Gesichtserkennung herangezogen.

316 Zum technischen Hintergrund Kapitel I. E. III.

317 BVerfGE 150, 244 (265).

318 BVerfGE 150, 244 (265) unter Verweis auch auf BVerfGE 65, 1 (42); 118, 168 (184 ff.); 120, 378 (400 f.); 128, 1 (42 ff.); 130, 151 (184).

319 Der Personenbezug ist hier sogar noch stärker, da sich das Embedding einer Person direkt aus deren persönlichen Merkmalen ergibt und sich ihr unmittelbar zuordnen

verknüpft; sie lassen sich demnach eindeutig einer identifizierten oder identifizierbaren Person zuordnen[320] und sind daher personenbezogen.[321] Die Embeddings (und der Gesichtserkennungsvorgang) unterfallen damit dem Schutzbereich der informationellen Selbstbestimmung.

2. Eingriffe und Intensität

Im nächsten Schritt ist danach zu fragen, welche einzelnen Schritte beim Einsatz von Gesichtserkennung[322] zur Ermittlung der Identität eines Tatverdächtigen Eingriffe darstellen und daher gerechtfertigt werden müssen. Zudem wird in diesem Abschnitt das Gewicht dieser Eingriffe bestimmt, da dies entscheidend dafür ist, welche Anforderungen an eine Rechtfertigung zu stellen sind.

a) Eingriff

Jeder staatliche Umgang mit – also die Verarbeitung von – personenbezogenen Daten bedeutet grundsätzlich einen Eingriff in das Recht auf informationelle Selbstbestimmung, denn jedes Mal wird es dem Betroffenen verwehrt, selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu entscheiden. Eine Erheblichkeitsschwelle besteht nicht.[323] Der Umgang mit personenbezogenen Daten durch staatliche Behörden begründet daher in der Regel verschiedene, aufeinander aufbauende Eingrif-

lässt, während sich mit dem Autokennzeichen nur mittelbar ein Personenbezug herstellen lässt (vgl. auch BVerfGE 150, 244 (280)).

320 Zutreffend *Schindler*, Biometrische Videoüberwachung, 303 f.

321 So auch *Schindler*, Biometrische Videoüberwachung, 304; *Hornung/Schindler*, DuD 2021, 515, 517. Vgl. zur Ebene des einfachen Rechts bereits *Hornung*, DuD 2004, 429 und zur Diskussion *Sofiotis*, VR 2010, 186, 187.

322 Zum Eingriff durch staatliche Videoüberwachung als solche *Schindler*, Biometrische Videoüberwachung, 306 ff. Zu Bild- und Videoaufnahmen, auf denen Personen identifizierbar aufgenommen wurden, als personenbezogene Daten, die in den Schutzbereich des Rechts auf informationelle Selbstbestimmung fallen, *ders.*, 292 ff.; überzeugend gegen eine Eröffnung des Schutzbereichs des Rechts auf informationelle Selbstbestimmung allein durch Einschüchterung und Überwachungsdruck *ders.*, 300 f.

323 *Kube*, in: Isensee/Kirchhof, Handbuch des Staatsrechts, Band VII, 3. Aufl. 2009, § 148 Rn. 81.

fe.[324] Insbesondere ist insoweit zwischen der Erhebung[325], Speicherung[326] und Verwendung[327] (insbesondere Übermittelung an andere Behörden[328]) von Daten zu unterscheiden.[329] Ein Eingriff ist auch der Abgleich von Daten, also der Vorgang, zwei (oder mehr)[330] Datensätze auf Übereinstimmungen oder Unterschiede zu untersuchen.[331]

Die Speicherung der Lichtbilder in einer Datenbank sowie die Heranziehung und Speicherung der Bild- oder Videoaufnahme eines Verdächtigen stellen somit Eingriffe in das Recht auf informationelle Selbstbestimmung dar.[332] Diese sind jedoch unabhängig von einer Verwendung dieser Bilder *zur Gesichtserkennung*. Die entscheidende Frage im Rahmen des Einsatzes von Gesichtserkennung ist daher, welche zusätzlichen rechtfertigungsbedürftigen Eingriffe sich aus diesem Vorgang ergeben.

---

324 Nach BVerfGE 100, 313 (366 f.); 115, 320 (343 f.); 120, 378 (400 f.); 125, 260 (310); 130, 151 (184); stRspr begründen „*Vorschriften*, die zum Umgang mit personenbezogenen Daten durch staatliche Behörden ermächtigen, […] in der Regel verschiedene, aufeinander aufbauende Eingriffe in das Recht auf informationelle Selbstbestimmung" (Hervorhebung J. H.). Wenn aber bereits die Vorschriften einen Eingriff bedeuten, dann erst recht auch die tatsächliche Vornahme dieser Verarbeitungsschritte.

325 Im Rahmen der DSGVO wird Erheben als das Beschaffen von Daten verstanden, Paal/Pauly/*Ernst*, 3. Aufl. 2021, DS-GVO Art. 4 Rn. 23, vgl. § 3 Abs. 3 BDSG aF.

326 Im Rahmen der DSGVO meint Speicherung das Aufbewahren, insbesondere auf einem Datenträger, zum Zwecke der weiteren Verarbeitung, Paal/Pauly/*Ernst*, 3. Aufl. 2021, DS-GVO Art. 4 Rn. 32.

327 Verwendung wird im Rahmen der DSGVO als Auffangtatbestand verstanden und soll alle Arten des zweckgerichteten Gebrauches oder der internen Nutzung von Daten erfassen, die von den übrigen Beispielen für Datenverarbeitungsschritte nicht umfasst sind, Paal/Pauly/*Ernst*, 3. Aufl. 2021, DS-GVO Art. 4 Rn. 29.

328 Besonders deutlich etwa BVerfGE 163, 43 (77 f.).

329 BVerfGE 100, 313 (366 f.); 115, 320 (343 f.); 120, 378 (400 f.); 125, 260 (310); stRpr.

330 Sydow/Marsch DS-GVO/BDSG/*Reimer*, 3. Aufl. 2022, DS-GVO Art. 4 Rn. 72.

331 *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, DSGVO Art. 4 Nr. 2, Rn. 27.

332 Die Speicherung von personenbezogenen Daten nennt das Bundesverfassungsgericht ausdrücklich als typischen Eingriff, vgl. nur z. B. BVerfGE 100, 313 (366 f.); 115, 320 (343 f.); 120, 378 (400 f.); 125, 260 (310). Für die Speicherung der Lichtbilder selbst muss eine eigene Rechtsgrundlage bestehen, was für die in INPOL gespeicherten Bilder regelmäßig der Fall ist, siehe etwa § 16 Abs. 1 S. 1 und 2, Abs. 5 AsylG oder § 81b Alt. 2 StPO. Allerdings wurde etwa die Datei Gewalttäter Sport jahrelang ohne Rechtsgrundlage betrieben, BVerwG, NJW 2011, 405; s. auch *Arzt*, NJW 2011, 352; *Arzt/Eier*, DVBl 2010, 816. Zu Recht kritisch auch zu der bedenklich weit gefassten Vorschrift des § 16 Abs. 5 AsylG Bergmann/Dienelt/*Bergmann*, 14. Aufl. 2022, AsylG § 16 Rn. 22; dagegen etwa BeckOK AuslR/*Houben*, 39. Ed., Stand: 1.10.2023, AsylG § 16 Rn. 20c.

Zur Ermittlung der Identität eines unbekannten Verdächtigen mittels Gesichtserkennung sind die folgenden Verarbeitungsschritte erforderlich: Zunächst müssen die Bilder in der zu durchsuchenden Lichtbilddatenbank für die Technologie durchsuchbar gemacht werden; hierfür erstellt das System für jede Person ein Embedding, also eine numerische Darstellung der Gesichtsmerkmale.[333] Auch aus den Merkmalen der unbekannten Person (auf dem zur Strafverfolgungsbehörde gelangten Lichtbild) muss ein Embedding erzeugt werden. Dieses gleicht das System dann mit allen anderen Embeddings ab und generiert eine Liste mit Treffern, die von Menschen überprüft werden.

aa) Eingriff durch Erstellung der Embeddings

Der erste Eingriff liegt bereits in der Erstellung und Speicherung[334] der Embeddings.[335] Denn dadurch werden die Lichtbilder maschinell durchsuchbar und in Sekundenschnelle auffindbar gemacht.

Schindler verneint hier einen eigenständigen Eingriff, wenn die Lichtbilder zusammen mit den aus ihnen erzeugten Embeddings in einer Datenbank gespeichert werden, da die Embeddings „auf das Wesentliche reduzierte Versionen dieser Lichtbilder" seien und „in ihrem Informationsgehalt

333 Zum Ablauf des Erkennungsvorgangs mit automatisierter Gesichtserkennung Kapitel I. E. III.

334 *Schindler*, Biometrische Videoüberwachung, 304 Fn. 1535 weist zutreffend darauf hin, dass es auch möglich wäre, die Embeddings/Templates für jeden Suchvorgang neu zu berechnen, dass dies jedoch mit einem unnötigen Ressourcenaufwand (Rechenleistung und Zeitaufwand) einhergeht.

335 So wohl auch *Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit*, Tätigkeitsbericht 2018, 87 f., der die „Verarbeitung von Abbildungen menschlicher Gesichter zu biometrischen Gesichtsmodellen" als erheblichen datenschutzrechtlichen Verstoß ansieht und von einem intensiven Eingriff in das Recht auf informationelle Selbstbestimmung spricht. Siehe auch *Stettner*, Sicherheit am Bahnhof, 2017, 146 (Generierung von Templates als eigenständiger Eingriff); BeckOK DatenschutzR/*Albers/Schimke*, 46. Ed., Stand: 1.8.2023, BDSG § 48 Rn. 11. Nicht ganz eindeutig insoweit *Kulick*, NVwZ 2020, 1622, 1623 („Das Erstellen eines Gesichtsprofils (Template) *und* der anschließende Abgleich mit einer Datenbank der Profile gesuchter Personen […] stellt *einen Eingriff* in ihr Recht auf informationelle Selbstbestimmung dar.") (Hervorhebung J. H.). Ebenso nicht ganz eindeutig bei *Heldt*, MMR 2019, 285, 287 (Vom Recht auf informationelle Selbstbestimmung „umfasst ist jedermanns äußerliche Erscheinung, sodass die biometrische Erfassung dessen – so wie eingangs dargestellt – zweifelsohne einen Eingriff durch den Staat darstellt.").

nicht über diese hinausgehen".[336] Diese Auffassung erscheint jedoch nicht überzeugend. Die zusätzliche (über die Speicherung des Lichtbilds) hinausgehende Beeinträchtigung der informationellen Selbstbestimmung liegt bei der Erstellung und Speicherung eines Embeddings darin, dass das Bild damit auf einen Schlag in Sekundenschnelle auch ohne den Namen des Betroffenen auffindbar gemacht wird. Die Speicherung eines *Lichtbilds* in einer großen Datenbank bedeutet, das Bild in ein Datenmeer hineinzuwerfen; die Erstellung und Speicherung eines *Embeddings* bedeutet hingegen, das Bild so zu markieren, dass es in Sekundenschnelle herausgefischt werden kann.

Bereits die Speicherung der Embeddings, wodurch die Lichtbilder per Gesichtserkennung durchsuchbar werden, begründet die erhöhte Gefahr, dass die Lichtbilder tatsächlich durchforstet werden und womöglich weitere Maßnahmen folgen. Die Umwandlung bildet die Basis für einen nachfolgenden Abgleich,[337] der nunmehr auch ohne den Namen des Betroffenen möglich ist. Das Grundrecht auf informationelle Selbstbestimmung will auch bereits *Gefährdungen* der Verhaltensfreiheit und Privatheit erfassen;[338] es genügt daher, dass die Daten abruf*bar* sind, sie müssen nicht tatsächlich abgerufen werden.

Das Argument, die Analyse der Gesichtsmerkmale und die Erstellung der Embeddings seien Vorgänge, die aus technischer Sicht notwendig seien, um die für die Gesichtserkennung benötigten biometrischen Merkmale zu extrahieren,[339] erscheint ebenfalls nicht zwingend. Auch die Speicherung von Daten ist aus technischer Sicht meist notwendig für eine Verwendung; dennoch sieht das Bundesverfassungsgericht auch dann einen selbstständigen Eingriff in der Speicherung, wenn die Daten ohnehin auch verwendet werden. Zudem ist denkbar, dass eine Regelung beispielsweise vorsieht, dass für Delikte unterschiedlicher Schwere jeweils verschiedene Datenbanken durchsucht werden dürften. Dann ist aber bereits die Erstellung von

336 *Schindler*, Biometrische Videoüberwachung, 312 f. spricht von einem „einheitlichen Eingriff", siehe auch *ders.*, 314 f.; kritisch hierzu *Arzt*, DÖV 2022, 866, 867.

337 Vgl. auch die Formulierung des Bundesverfassungsgerichts „Ein Eingriff liegt insoweit grundsätzlich zunächst in der Erfassung personenbezogener Daten. Sie macht die Daten für die Behörden verfügbar und bildet die Basis für einen nachfolgenden Abgleich mit Suchbegriffen." z. B. in BVerfGE 120, 378 (398); 150, 244 (266); ähnlich auch BVerfGE 100, 313 (366).

338 Vgl. nur BVerfGE 150, 244 (264); vgl. auch *Bäcker*, Der Staat 2012, 91, 94 ff.; *Poscher*, in: Gander/Perron/Poscher/Riescher/Würtenberger, Resilienz in der offenen Gesellschaft, 2012, 167, 174 ff.

339 *Schindler*, Biometrische Videoüberwachung, 315.

Embeddings und damit die Entscheidung, dass diese Personen *überhaupt* (je nach Fallkonstellation) gescannt werden dürfen, eine Beeinträchtigung ihrer informationellen Selbstbestimmung. Anderenfalls würde es auch keinen rechtfertigungsbedürftigen Eingriff begründen, aus den Personalausweisfotos aller Bürgerinnen und Bürger Embeddings zu erstellen und diese auf Vorrat zu halten, um sie – im Falle der Schaffung einer passenden Rechtsgrundlage – dann für Abgleiche heranzuziehen.

Daran ändert auch der Umstand nichts, dass, wie sogleich besprochen wird, auch der Abgleich der Embeddings einen Eingriff darstellt. Um im Bild zu bleiben: Mit der Speicherung eines *Embeddings* wurde das Bild so markiert, dass es in Sekundenschnelle aus einem Datenmeer herausgefischt werden kann; mit dem *Abgleich* entscheidet die Strafverfolgungsbehörde, welche Embeddings (z. B. welche Datenbank) abgeglichen werden sollen und damit an welcher Stelle des Datenmeers überhaupt gefischt werden soll.

bb) Eingriff durch Abgleich

Auch der Abgleich der Embeddings als solcher begründet als „Akt der Auswahl für eine weitere Auswertung“[340] einen eigenständigen Eingriff in das Recht auf informationelle Selbstbestimmung.[341] Betroffen sind dabei alle Personen, deren Embeddings in den Abgleich einbezogen werden, insbesondere auch die „Nichttreffer“.

Aufschlussreich ist in dieser Hinsicht die Rechtsprechung des Bundesverfassungsgerichts zu automatisierten Kfz-Kennzeichenkontrollen.[342] Eine *direkte* Parallele zwischen der automatisierten Kfz-Kennzeichenkontrolle und dem Einsatz von Gesichtserkennung besteht mit Blick auf das (in dieser Arbeit nicht vertieft behandelte) Einsatzszenario der Echtzeit-Fahndung[343]. In beiden Fällen werden in Echtzeit vorbeifahrende Autos bzw. vorbeilaufende Personen erfasst und mit einem Fahndungsbestand abgeglichen. Dagegen

340 Siehe nur BVerfGE 115, 320 (344); 100, 313 (366).

341 Zum Abgleich von personenbezogenen Daten als Eingriff BVerfGE 115, 320 (344) u. BVerfGE 100, 313 (366). Speziell zum Abgleich bei Gesichtserkennung als Eingriff *Schindler*, Biometrische Videoüberwachung, 313; so wohl auch *Martini/Thiessen/Ganter*, Digitale Versammlungsbeobachtung, 2023, 110; *Kulick*, NVwZ 2020, 1622, 1623; *Stettner*, Sicherheit am Bahnhof, 2017, 146; *Thiel*, ZRP 2016, 218, 219.

342 BVerfGE 150, 244.

343 Zu diesem Szenario Kapitel I. C. II. 4.

wird in dem in dieser Arbeit betrachteten – und in der Praxis in Deutschland bereits Realität gewordenen – Szenario der Identitätsfeststellung zum einen erst im Nachhinein abgeglichen, zum anderen werden nicht alle Passanten gescannt, sondern „nur" die Personen, die in einer (erkennungsdienstlichen) Datenbank gespeichert sind. An der Frage, ob überhaupt ein *Eingriff* vorliegt, ändert dies jedoch nichts,[344] die Rechtsprechung des Bundesverfassungsgerichts zu automatisierten Kfz-Kennzeichenkontrollen kann hier herangezogen werden.

In dieser Entscheidung kam das Gericht – unter Aufgabe seiner früheren Rechtsprechung[345] – zu dem Schluss, dass es für das Vorliegen eines Eingriffs in das Grundrecht auf informationelle Selbstbestimmung nicht darauf ankommt, ob sich als Ergebnis der Kontrolle ein Trefferfall ergibt oder nicht.[346] Auch wenn die Kontrolle zu einem Nichttreffer führt, liegen demnach in der Erfassung und dem Abgleich des Kfz-Kenneichens Eingriffe. Denn mit dem Abgleich würden die Betroffenen „einer staatlichen Maßnahme unterzogen […], mit der sich ihnen gegenüber ein spezifisches Fahndungsinteresse zur Geltung bringt".[347]

Abzulehnen sei ein Grundrechtseingriff in der Regel lediglich dann, wenn „personenbezogene Daten Dritter im Rahmen von elektronischen Datenverarbeitungsprozessen nur zufällig am Rande miterfasst werden und unmittelbar nach der Erfassung technisch wieder anonym, spurenlos und ohne Erkenntnisinteresse für die Behörden gelöscht werden".[348] Ein Eingriff sei insoweit nur anzunehmen, wenn sich das behördliche Interesse an den betroffenen Daten „spezifisch verdichtet" hat.[349] Dazu führte das Bundesverfassungsgericht aus:[350]

> „Unter den Bedingungen der modernen Informationstechnik, die den Abgleich von Kennziffern oder persönlichen Merkmalen mit großen Datenmengen in kürzester Zeit erlauben, ist bei Kontrollvorgängen wie vorliegend der Kennzeichenkontrolle eine solche Verdichtung gegeben. Wenn gezielt mittels Datenabgleich Personen im öffentlichen Raum dar-

344 Der Umstand, dass ein Abgleich mit weniger Personen stattfindet, kann hingegen beim Eingriffsgewicht eine Rolle spielen, wie sogleich noch erörtert wird, siehe Kapitel II. A. I. 2. b).
345 BVerfGE 120, 378.
346 BVerfGE 150, 244 (266).
347 BVerfGE 150, 244 (268).
348 BVerfGE 150, 244 (266 f.); siehe auch bereits BVerfGE 100, 313 (366); 115, 320 (343).
349 BVerfGE 150, 244 (266 f.).
350 BVerfGE 150, 244 (267 f.).

aufhin überprüft werden, ob sie oder die von ihnen mitgeführten Sachen polizeilich gesucht werden, besteht an deren Daten auch dann ein verdichtetes behördliches Interesse, wenn diese Daten im Anschluss an die Überprüfung unmittelbar wieder gelöscht werden.
Maßgeblich ist hierfür, dass Erfassung und Abgleich der Daten einen Kontrollvorgang begründen, der sich bewusst auf alle in die Kennzeichenkontrolle einbezogenen Personen erstreckt und erstrecken soll. Die Einbeziehung der Daten auch von Personen, deren Abgleich letztlich zu Nichttreffern führt, erfolgt nicht ungezielt und allein technikbedingt, sondern ist notwendiger und gewollter Teil der Kontrolle und gibt ihr als Fahndungsmaßnahme erst ihren Sinn. In der ex ante-Perspektive der Behörde, die für die Einrichtung einer Kennzeichenkontrolle maßgeblich ist, besteht ein spezifisch verdichtetes Interesse daran, die Kennzeichen aller an der Kennzeichenerfassungsanlage vorbeifahrenden oder sonst in die Kontrolle einbezogenen Fahrzeuge zu erfassen, weil es gerade um deren Kontrolle selbst geht. Zu diesem Zweck werden die Daten gezielt erhoben und kommt es auch auf deren Zuordenbarkeit zu den jeweiligen Personen an. Dass deren Auswertung automatisiert erfolgt, stellt dies nicht in Frage; vielmehr werden damit die Kontrollmöglichkeiten der Polizei wesentlich erweitert." (Hervorhebung J. H.)

So liegt der Fall auch und erst recht bei der Verwendung von Gesichtserkennung zum Abgleich der Embeddings aller in einer Datenbank gespeicherten Personen mit dem Embedding des unbekannten Tatverdächtigen. Es besteht ein verdichtetes behördliches Interesse an den Daten aller in der Datenbank erfassten Individuen, weil gerade ermittelt werden soll, ob einer oder eine von ihnen der Verdächtige ist (bzw. mit dem Verdächtigen übereinstimmende Gesichtsmerkmale aufweist).

Dem steht auch nicht entgegen, dass bei der automatisierten Kfz-Kennzeichenkontrolle die vorbeifahrenden Pkw gerade wegen der Kontrolle aufgezeichnet werden, während bei der Verwendung von Gesichtserkennung zur Identitätsermittlung Bilder (bzw. daraus generierte Embeddings) abgeglichen werden, die zuvor ohnehin bereits in der Datenbank gespeichert waren und unter anderem dem Zweck dienten, unbekannte Verdächtige zu identifizieren. Dies könnte für die Bestimmung des Eingriffsgewichts relevant sein;[351] für die Frage, ob ein Eingriff vorliegt, gilt jedoch, dass zwischen der Erhebung und Verarbeitung personenbezogener Daten gerade

351 Hierzu Kapitel II. A. I. 2. b).

differenziert werden soll und daher jeweils eigenständige Eingriffe vorliegen.

Auch ist ein Eingriff nicht deshalb abzulehnen, weil ein Mensch (z. B. Polizeibeamter) ohne Weiteres analog eine Kartei mit Lichtbildern durchblättern dürfte und so versuchen könnte, den Verdächtigen zu identifizieren. Denn das besondere Eingriffspotenzial von Maßnahmen der elektronischen Datenverarbeitung liegt gerade in der Menge der verarbeitbaren Daten, die auf konventionellem Wege gar nicht bewältigt werden könnte.[352] Die Schnelligkeit und Menge an bewältigbaren Daten bei einem Abgleich per Gesichtserkennung ist mit menschlichen Fähigkeiten nicht zu vergleichen. Dieser Unterschied in der Quantität ist so immens, dass er damit auch einen Unterschied in der *Qualität* der Datenverarbeitung bewirkt.[353]

cc) Eingriff durch Treffer

Führt der Abgleich dazu, dass eine Person in die Kandidatenliste mit möglichen Übereinstimmungen aufgenommen wird („Treffer"), so liegt hierin ein Eingriff.[354] Durch einen (echten) Treffer können neue Erkenntnisse gewonnen werden. Zum einen können Name und Adresse der unbekannten Person sowie weitere Informationen über sie herausgefunden werden.[355] Zum anderen kann erkannt werden, wo sich eine (durch die Datenbank namentlich bekannte) Person aufgehalten hat und was sie gemacht hat, denn diese Information enthält das von der Polizei oder Privaten angefertigte Lichtbild, das zum Abgleich herangezogen wird.[356]

Daran ändert auch der Umstand nichts, dass nicht unmittelbar ein eindeutiger „Treffer" gemeldet, sondern nur eine Kandidatenliste mit meh-

352 BVerfGE 120, 378 (397 f.) mwN; stRspr.

353 Hierzu bereits oben Kapitel II. A. I. am Anfang.

354 *Schindler*, Biometrische Videoüberwachung, 313. Siehe zu Gesichtserkennung bereits *Zöller*, NVwZ 2005, 1235, 1238 („zumindest ein Eingriff der handelnden Polizeibehörde in das informationelle Selbstbestimmungsrecht derjenigen Personen, die bei einer solchen Rasterung als ‚Treffer' vom Computersystem angezeigt werden").

355 *Schindler*, Biometrische Videoüberwachung, 313.

356 Dies gilt nicht nur dann, wenn auf dem Bild unmittelbar der Ort der Aufnahme ersichtlich ist, sondern grundsätzlich für alle digitalen Fotos, da sie zusätzliche Informationen enthalten (sog. Exif-Daten), z. B. über den Ort und die Zeit ihrer Aufnahme.

reren möglichen Übereinstimmungen generiert wird[357] und ein Mensch die letztendliche Entscheidung darüber trifft, ob sich die gesuchte Person unter den ermittelten Kandidaten befindet. Denn für die Eingriffsqualität kommt es nach der Rechtsprechung nicht darauf an, ob eine Auswahl maschinell oder durch einen Menschen erfolgt.[358] Dann muss ein Eingriff erst recht gegeben sein, wenn die Technologie bereits eine konkrete Vorauswahl in Form einer Kandidatenliste getroffen hat und dann zusätzlich noch ein Mensch auswählt. Auch mit Blick auf die automatisierten Kfz-Kennzeichenkontrollen wurde ein Eingriff nicht etwa deshalb abgelehnt, weil Polizeibeamte die vom Computer gemeldete Übereinstimmung visuell überprüften.[359]

Auch bei falschen Treffern (False positives) ist ein Eingriff anzunehmen. Die gegenteilige Auffassung hatte noch das Bundesverwaltungsgericht vor der verfassungsgerichtlichen Entscheidung Automatisierte Kfz-Kennzeichenkontrolle II vertreten.[360] Zwar werde das erfasste Kennzeichen in dieser Konstellation durch den Polizeibeamten, der mit dem visuellen Abgleich betraut ist, zur Kenntnis genommen. Der Polizeibeamte beschränke sich jedoch auf die Vornahme dieses Abgleichs und lösche den Vorgang umgehend, wenn der Abgleich negativ ausfalle; daher sei das behördliche Interesse ist in diesem Stadium nur ein „systembezogenes Korrekturinter-

357 Es ließe sich daher darüber diskutieren, ob der Begriff „Treffer" in diesem Einsatzszenario von Gesichtserkennung passend ist. Aus technologischer Sicht handelt es sich jedoch um einen Treffer, denn er entspricht den gewählten Kriterien wie Ähnlichkeitsschwelle usw.

358 BVerfGE 100, 313 (366) (zu Art. 10 GG): „Dem Abgleich selbst kommt als Akt der Auswahl für die weitere Auswertung Eingriffscharakter zu. Das gilt unabhängig davon, ob er maschinell vor sich geht oder durch Mitarbeiter des Bundesnachrichtendienstes erfolgt, die zu diesem Zweck den Kommunikationsinhalt zur Kenntnis nehmen.". Hierbei ging es zwar um den *Abgleich* als solchen, nicht die letztendliche Auswahl. Da die letztendliche Auswahl aber mit noch höherer Wahrscheinlichkeit mit Folgemaßnahmen einhergeht, muss diese Aussage des Bundesverfassungsgerichts erst recht auch für diesen Akt gelten.

359 Zum Vorgehen bei automatisierten Kfz-Kennzeichenkontrollen BVerfGE 150, 244 (251): „Polizeibeamte überprüfen visuell, ob das aufgenommene Bild des Kraftfahrzeugkennzeichens und das im Fahndungsbestand gespeicherte Kraftfahrzeugkennzeichen übereinstimmen. Bestätigt die visuelle Überprüfung die vom Computer gemeldete Übereinstimmung nicht (unechter Trefferfall), gibt ein Polizeibeamter durch Betätigen der Taste ‚Entfernen' den Befehl, den gesamten Vorgang zu löschen. Sofern die Überprüfung einen Treffer bestätigt (Trefferfall), werden diese Daten gespeichert und gegebenenfalls weitere polizeiliche Maßnahmen in die Wege geleitet."

360 BVerwG, NVwZ 2015, 906, 908.

esse".[361] Das Bundesverfassungsgericht geht in seiner anschließenden Entscheidung auf diese Fallkonstellation gar nicht gesondert ein, da es ohnehin bereits mit Blick auf den Abgleich (also sogar für die Nichttreffer) einen Eingriff annimmt.[362]

Die Auffassung, dass bei falschen Treffern ein Eingriff abzulehnen sei, ist jedoch auch in der Sache abzulehnen, insbesondere bei der Verwendung von Gesichtserkennung. Denn bereits das Auftauchen in der Liste konkretisiert das behördliche Interesse an den Daten der betroffenen Person näher und begründet zudem die konkrete Gefahr für Folgemaßnahmen. Dies gilt nicht zuletzt deshalb, weil die Identifizierung von Menschen anhand von Lichtbildern fehleranfällig ist. Sowohl der Maschine als auch dem überprüfenden Polizeibeamten können Fehler unterlaufen, sodass ein Unschuldiger als Verdächtiger identifiziert werden kann. Dass dies nicht nur eine theoretische Gefahr ist, wird besonders deutlich bei einem Blick auf die Fälle der Festnahmen Unschuldiger in den USA nach falschen Gesichtserkennungs-Matches.[363] Dabei ist Gesichtserkennung in gewisser Hinsicht noch deutlich fehleranfälliger als die automatisierte Kfz-Kennzeichenkontrolle.[364] Bereits bei der automatisierten Kfz-Kennzeichenkontrolle sind Fehler möglich;[365] im Zeitraum Juni bis September 2011 wurden in Bayern etwa 40.000 bis 50.000 Treffermeldungen generiert, davon waren aber nur 500 bis 600 echte Treffer.[366] Hier können falsche Treffer aber leichter dadurch erkannt werden, dass im Rahmen der menschlichen Überprüfung der Treffer lediglich Buchstaben und Ziffern (das Kennzeichen) abgeglichen werden müssen. Bei der Gesichtserkennung ist ein Abgleich weniger eindeutig. Die Fehleranfälligkeit von Gesichtserkennung wird zwar deutlich reduziert, wenn – wie beim BKA und den Landeskriminalämtern praktiziert – Experten (hierzu näher unten) die letztendliche Identifizierung vornehmen. Aber auch diese können Fehler machen. Und wenn ledig-

361 BVerwG, NVwZ 2015, 906, 908.
362 BVerfGE 150, 244 (266).
363 Hierzu bereits Kapitel I. G. II. 1. A) und ausführlich Kapitel III. B. Zwar dürfen diese Fälle nicht unkritisch auf Deutschland übertragen werden. Das Bundesverfassungsgericht argumentiert jedoch selbst (auch etwa im Hinblick auf Missbrauchsgefahren) regelmäßig auch dann mit dem „worst case", wenn nicht naheliegt, dass dieser in absehbarer Zeit in Deutschland eintritt, siehe nur BVerfG, NJW 2023, 3698, 3708.
364 Zur Fehleranfälligkeit von Gesichtserkennung und den Ursachen für Fehler auf technischer Ebene Kapitel I. E. IV., zu menschlichen Ursachen für Fehler Kapitel III. B. II. 2.
365 Zu möglichen Gründen für Fehler LT-Drs. SN 6/8121, 2.
366 BVerfGE 150, 244 (252).

lich ein Bild von schlechter Qualität vorliegt, können auch die Experten nur einen „Verdacht" der Personenidentität äußern; dieser müsste dann durch weitere Ermittlungen überprüft werden und kann sich als unzutreffend erweisen.

dd) Fazit

Der Einsatz von Gesichtserkennung zur Ermittlung der Identität unbekannter Verdächtiger begründet Eingriffe in das Recht auf informationelle Selbstbestimmung. Ein Eingriff ist dann anzunehmen, wenn eine Person auf der Kandidatenliste erscheint („Treffer"). Aber auch bereits die Erstellung der Face Embeddings sowie der Abgleich mit den Embeddings aller in der Datenbank gespeicherten Personen begründen eigenständige Eingriffe, die rechtfertigungsbedürftig sind. Betroffen ist insoweit die informationelle Selbstbestimmung aller Personen, die in einer zur Gesichtserkennung verwendeten Datenbank gespeichert sind.

b) Erhebliches Eingriffsgewicht

Im nächsten Schritt ist nach der Intensität der Eingriffe zu fragen.[367] Diese bestimmt vor allem, welche Anforderungen an die Verhältnismäßigkeit sowie an die Bestimmtheit und Normenklarheit zu stellen sind.

Das Eingriffsgewicht orientiert sich an den tatsächlichen Wirkungen einer Maßnahme und ihrer normativen Bewertung.[368] Für seine Bestimmung haben sich in der Rechtsprechung des Bundesverfassungsgerichts

367 Das Bundesverfassungsgericht spricht mit Blick auf die Intensität eines Eingriffs etwa von einem „erheblichen" (z. B. BVerfGE 150, 244 (284)), „erhöhten" (z. B. BVerfGE 155, 119 (200)), „hohen" (z. B. BVerfG, NVwZ 2007, 688 (691)), „besonders hohen" (z. B. BVerfGE 155, 119 (229)), „besonders schweren" (BVerfGE 162, 1 (161)), „außerordentlichen" BVerfGE 162, 1 (108) oder auch „speziellen" (BVerfGE 162, 1 (74)) Eingriffsgewicht. Eine genaue Abgrenzung ist nicht ersichtlich und aufgrund der unterschiedlichen Natur der Eingriffe in das Recht auf informationelle Selbstbestimmung auch nicht allgemeingültig möglich. Zu einem möglichen vierstufigen Modell *Bäcker*, in: Herdegen/Masing/Poscher/Gärditz, Handbuch des Verfassungsrechts, 2021, § 28 Sicherheitsverfassungsrecht, Rn. 93.

368 *Schwabenbauer*, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, Kapitel G. Informationsverarbeitung im Polizei- und Strafverfahrensrecht, Rn. 119.

und in der Literatur verschiedene Kriterien herausgebildet.[369] Die Kategorien ergänzen und überschneiden sich teilweise. Die Intensität des Eingriffs wird vor allem durch Art, Umfang und denkbare Verwendung der Daten sowie die Gefahr ihres Missbrauchs bestimmt.[370] Dabei ist unter anderem bedeutsam, wie viele Grundrechtsträger wie intensiven Beeinträchtigungen ausgesetzt sind und unter welchen Voraussetzungen dies geschieht, insbesondere ob diese Personen hierfür einen Anlass gegeben haben.[371] Maßgebend sind also die Gestaltung der Eingriffsschwellen, die Zahl der Betroffenen und die Intensität der individuellen Beeinträchtigung im Übrigen.[372] Für das Gewicht der individuellen Beeinträchtigung ist erheblich, ob die Betroffenen als Personen anonym bleiben, welche persönlichkeitsbezogenen Informationen erfasst werden und welche Nachteile den Grundrechtsträgern aufgrund der Maßnahmen drohen oder von ihnen nicht ohne Grund befürchtet werden.[373] Dabei führt insbesondere die Heimlichkeit einer staatlichen Eingriffsmaßnahme zur Erhöhung ihrer Intensität,[374] ebenso wie die faktische Verwehrung vorherigen Rechtsschutzes und die Erschwerung nachträglichen Rechtsschutzes, wenn er überhaupt zu erlangen ist[375].

Im Folgenden werden die Faktoren herausgearbeitet, die beim Einsatz von Gesichtserkennung zur Identitätsermittlung bei unbekannten Verdächtigen das Eingriffsgewicht erhöhen; zudem wird ein eigener Vorschlag für ein weiteres relevantes Kriterium unterbreitet. Auch wird untersucht, welche Umstände das Eingriffsgewicht bei dieser Maßnahme abmildern.

369 Zu diesen kritisch etwa Sondervotum Haas, BVerfGE 115, 320 (371). Zu den Kriterien etwa auch *Schwabenbauer*, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, Kapitel G. Informationsverarbeitung im Polizei- und Strafverfahrensrecht, Rn. 119 ff.; *Martini*, in: Emmenegger/Wiedmann, Linien der Rechtsprechung des Bundesverfassungsgerichts – erörtert von den wissenschaftlichen Mitarbeitern, 2011, 301, 315 ff.; *Tanneberger,* Die Sicherheitsverfassung, 2014, 232 ff., auch mit dem Versuch einer Systematisierung.

370 Vgl. BVerfGE 65, 1 (45 f.); 155, 119 (178); siehe auch BVerfGE 165, 363 (399 ff.).

371 BVerfGE 155, 119 (178).

372 BVerfGE 165, 363 (399).

373 BVerfGE 115, 320 (347).

374 BVerfGE 155, 119 (179) mwN.

375 BVerfGE 113, 348 (383 f.); 118, 168 (197 f.); 120, 378 (403).

aa) Heimlichkeit

Maßnahmen, die heimlich – also ohne Wissen der Betroffenen – durchgeführt werden, haben eine erhöhte Eingriffsintensität.[376] Sie erschweren den Rechtsschutz (vgl. Art. 19 Abs. 4 GG) und damit auch die Kontrolle durch Betroffene und die Öffentlichkeit.[377] Dadurch bergen heimliche Maßnahmen auch eine erhöhte Missbrauchsgefahr.[378] Zudem führen sie zu einem Mangel an Transparenz, da der Einzelne bei einer geheimen Datenverarbeitung nicht nachvollziehen kann, welche Informationen die Behörden über ihn haben.[379]

Der Einsatz von Gesichtserkennung zur Ermittlung der Identität unbekannter Verdächtiger erfolgt ohne Kenntnis der Betroffenen. Von der Maßnahme erfahren weder die Personen, deren Embeddings abgeglichen werden, noch die Person, die letztendlich als Tatverdächtiger identifiziert wurde. Erst zu einem späteren Zeitpunkt im Zuge der Ermittlungen (bei Beantragung von Akteneinsicht) oder im Rahmen der Hauptverhandlung erfährt der als Täter Identifizierte unter Umständen von der Verwendung von Gesichtserkennung. Zwar entspricht es jedenfalls im Zusammenhang mit Recherchen im BKA-GES der gängigen Praxis, einen Bericht über

376 BVerfGE 113, 348 (383 f.); 115, 320 (353); 118, 168 (197 f.); 141, 220 (265); vgl. auch EuGH, Urt. v. 21.12.2016, Tele2 Sverige und Watson u. a., C-203/15 u. a., EU:C:2016: 970, Rn. 100). Vgl. zum Ganzen näher auch *Schwabenbauer*, Heimliche Grundrechtseingriffe, 2013, 123 ff; zur Besonderheit heimlicher Maßnahmen etwa *Diggelmann*, VVDStRL 2011, 50, 73. Kritisch zum Kriterium der Heimlichkeit (Unkenntnis von der Maßnahme) Sondervotum Haas, BVerfGE 115, 320 (372), die hierin einen Widerspruch zum gleichzeitig vom Bundesverfassungsgericht herangezogenen Kriterium der Einschüchterungseffekte (Sorge vor und daher Wissen um die Maßnahme) sieht. Gegen diesen vermeintlichen Widerspruch überzeugend *Schindler*, Biometrische Videoüberwachung, 2021, 481.

377 Vgl. auch MüKoStPO/*Gaede*, 1. Aufl. 2018, EMRK Art. 8 Rn. 22. Zu weiteren Gründen dafür, warum bei heimlichen Maßnahmen eine erhöhte Eingriffsintensität besteht *Schwabenbauer*, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, Kapitel G. Informationsverarbeitung im Polizei- und Strafverfahrensrecht, Rn. 126 ff.

378 Vgl. auch zu diesem Gedanken EGMR, NJW 2007, 1433 (1435): „Insbesondere bei geheimer Ausübung einer der Exekutive zustehenden Befugnis ist […] die Gefahr der Willkür offensichtlich."

379 Vgl. etwa zur Vorratsdatenspeicherung BVerfGE 125, 260 (335): „Der Einzelne weiß nicht, was welche staatliche Behörde über ihn weiß, weiß aber, dass die Behörden vieles, auch Höchstpersönliches über ihn wissen können. Der Gesetzgeber muss die diffuse Bedrohlichkeit, die die Datenspeicherung hierdurch erhalten kann, durch wirksame Transparenzregeln auffangen."

die Recherche zu den Akten zu nehmen, deren Einsicht der Betroffene beantragen kann.[380] Gesetzlich geregelt ist eine Benachrichtigung allerdings nicht. Die Intensität einer Maßnahme ist im Übrigen auch dann erhöht, wenn eine Benachrichtigung zwar gesetzlich vorgesehen ist, aber erst nach Abschluss der Maßnahme erfolgt.[381]

Nicht entscheidend ist, dass die ursprüngliche erkennungsdienstliche Erfassung (einschließlich der Lichtbildaufnahme) mit Kenntnis des Betroffenen erfolgt ist. Auch ist unerheblich, ob die Aufzeichnung des unbekannten Verdächtigen durch eine offene Videoüberwachung oder ein offen erkennbares Fotografieren durch Polizeibeamte erfolgte. Denn die Verwendung von Gesichtserkennung ist eine davon unabhängige eigenständige Maßnahme. Wer weiß, dass er fotografiert wurde, weiß noch lange nicht, dass sein Gesicht später automatisiert abgeglichen wird.[382]

bb) Streubreite und Anlasslosigkeit

Eingriffserhöhend wirken auch die Streubreite (Vielzahl von Betroffenen) und die Anlasslosigkeit einer Maßnahme.[383] Denn der Einzelne ist in seiner grundrechtlichen Freiheit umso intensiver betroffen, je weniger er selbst für einen staatlichen Eingriff Anlass gegeben hat.[384] Anlasslos bedeutet dabei, dass Personen in den Wirkungsbereich einer Maßnahme einbezogen werden, die hierfür durch ihr Verhalten keinen Anlass gegeben haben.[385] Diese Frage ist gerade bei der Gesichtserkennung eine entscheidende Weichen-

380 Das gilt sowohl für (ausführliche) Untersuchungsberichte zur Personenidentität als auch für Kurzberichte, wenn lediglich ein ermittlungsunterstützender Hinweis vorliegt (Verdacht auf Personenidentität).

381 BVerfGE 115, 320 (353).

382 Ähnlich für den Kontext der Echtzeit-Fahndung auch *Schindler*, Biometrische Videoüberwachung, 2021, 507.

383 Vgl. BVerfGE 100, 313 (376, 392); 107, 299 (320 f.); 109, 279 (353); 113, 29 (53); 113, 348 (383); 115,320 (354). Zur bislang fehlenden näheren Konturierung des Begriffs der Streubreite *Rademacher*, JZ 2019, 702, 706 Fn. 45.

384 BVerfGE 115, 320 (354).

385 Vgl. etwa BVerfGE 120, 378 (411) („Personenkreis […], der durch sein Verhalten keinen Anlass für die Aufnahme in den Fahndungsbestand gegeben hat") und BVerfGE 107, 299 (320 f.) („Betroffen sind Personen, die selbst nicht verdächtig sind."); siehe auch BVerfGE 109, 279 (353); 113, 29 (53); 113, 348 (383); 115, 320 [354]); 150, 244 (283). Es ist damit nicht gemeint, dass aus Sicht der Polizei kein Anlass für die Maßnahme besteht, vgl. *Schindler*, Biometrische Videoüberwachung, 2021, 474. Allerdings erscheint es etwas unglücklich, dass das Bundesverfassungsgericht an anderer Stelle auch davon spricht, dass ein „Anlass" für die Maßnahme (als solche)

stellung für die Festlegung des Eingriffsgewichts. Dass der zu identifizierende unbekannte *Verdächtige* einen Anlass zum Abgleich gibt, erschließt sich ohne Weiteres, denn es steht im Raum, dass dieser eine Straftat begangen hat. Bei den zahlreichen *Personen in der Datenbank* ist jedoch fraglich, inwiefern diese einen Anlass für den Abgleich geben.

Wann ein zurechenbarer Anlass vorliegt, hat sich jedoch in der verfassungsgerichtlichen Judikatur noch nicht eindeutig herauskristallisiert. In der ersten Entscheidung zu automatisierten Kfz-Kennzeichenkontrollen erwähnt das Bundesverfassungsgericht nur am Rande, dass der Betroffene einen ihm zurechenbaren Anlass etwa durch eine „Rechtsverletzung" gebe.[386] Gemeint sind damit wohl solche Rechtsverletzungen, zu deren Aufklärung die Kennzeichenkontrollen durchgeführt werden, also etwa ein Autodiebstahl[387]. Es wird wohl kaum gemeint sein, dass jeder, der irgendwann einmal irgendeine Rechtsverletzung begangen hat, einen Anlass für die Kontrolle gibt.[388] In der Entscheidung zu automatisierten Datenanalysen spricht das Gericht von „Personen, die objektiv nicht zurechenbar in das relevante Geschehen verfangen sind"; auch das deutet darauf hin, dass eine Anlassbezogenheit nur besteht, wenn die Person mit der konkreten Situation im Zusammenhang steht.[389]

Mit Blick auf den Einsatz von Gesichtserkennung zur Identifizierung unbekannter Verdächtiger ist für die Frage der Streubreite und Anlasslosigkeit entscheidend, welche Datenbank zum Abgleich herangezogen wird.[390] Denn damit wird die Entscheidung getroffen, wessen personenbezogene

---

vorliegen muss, siehe etwa BVerfGE 120, 378 (419) („Anlass der Kennzeichenerfassung").

386 BVerfGE 120, 378 (402); hierzu etwa auch *Härtel*, LKV 2019, 49, 55. Teilweise formuliert das Bundesverfassungsgericht weiter und sieht es als intensitätserhöhend an, wenn ein Eingriff erfolgt, „ohne Anknüpfung an ein zurechenbar vorwerfbares Verhalten, eine – auch nur abstrakte – Gefährlichkeit oder sonst eine qualifizierte Situation.", BVerfGE 125, 260 (318).

387 *Frenz*, JA 2013, 840, 843.

388 Schließlich argumentiert das Bundesverfassungsgericht in den Entscheidungen zu automatisierten Kfz-Kennzeichenkontrollen (BVerfGE 150, 244 und BVerfGE 150, 244) nicht, dass etwa die zufälligerweise vorbeifahrenden Personen, die einer Straftat verdächtig sind oder die einmal eine Straftat begangen haben (aber deren Kennzeichen nicht auf der Fahndungsliste steht), einen Anlass für die Kontrolle gegeben hätten.

389 BVerfGE 165, 363 (398 f.).

390 Vgl. auch mit Blick auf automatisierte Kfz-Kennzeichenkontrollen BVerfGE 150, 244 (269), wonach „Art und Bedeutung der in den Abgleich einbezogenen Datenbestände" für die Bestimmung des Eingriffsgewichts entscheidend sind.

Daten (Embeddings) mit denen des Verdächtigen abgeglichen werden und daher welche und wie viele Personen von dem Eingriff betroffen sind. Mit dem Gesichtserkennungssystem GES des BKA können die in INPOL-Z gespeicherten Lichtbilder gescannt werden. Darunter sind insbesondere Aufnahmen von Personen, die wegen des Verdachts einer Straftat erkennungsdienstlich behandelt wurden, aber auch etwa alle Asylsuchenden.[391] 6,7 Millionen Porträtaufnahmen zu rund 4,6 Millionen Personen sind gespeichert. Das bedeutet eine erhebliche Streubreite. Der Abgleich (und auch bereits die Erstellung der Embeddings) betrifft zudem in erster Linie Personen, die hierfür keinen Anlass gegeben haben.

Wer wegen eines Ladendiebstahls in Oberbayern erkennungsdienstlich behandelt wurde, gibt noch lange keinen Anlass dafür, in einen Datenabgleich wegen eines Totschlags in Hamburg, dann wegen eines Betäubungsmitteldelikts in Frankfurt und dann wieder wegen eines Raubüberfalls in Köln einbezogen zu werden. Der Abgleich im GES erfolgt aber ohne Filter etwa nach Tatort oder Deliktsart; alle gespeicherten Personen werden abgeglichen. Es gibt jedoch keine auch nur ansatzweise konkreten Anhaltspunkte dafür, dass gerade einer von ihnen der unbekannte Verdächtige ist.[392]

Selbst wenn man in der Begehung irgendeiner (!) Straftat einen hinreichenden Anlass für die Einbeziehung in die Gesichtserkennungsrecherche sehen würde, darf nicht aus dem Blick geraten, dass der Abgleich zu einem großen Teil Personen erfasst, die lediglich einmal *verdächtigt* wurden, eine Straftat[393] begangen zu haben und in diesem Rahmen einer erkennungsdienstlichen Behandlung nach § 81b StPO unterzogen wurden, wenn die

391 Hierzu bereits Kapitel I. F. I. 1.

392 Anders *Schindler*, der der Auffassung ist, es liege bei den Personen, die der Gesichtserkennung unterworfen werden, „in Gestalt eines Straftatverdachts ein konkreter Grund vor" und es fehle der Maßnahme daher an der Streubreite, *Schindler*, Biometrische Videoüberwachung, 2021, 509. In diese Richtung wohl auch *Petri*, GSZ 2018, 144, 148. Mit Blick auf Datenverwendung im Rahmen von Predictive Policing sieht *Singelnstein* wohl ebenfalls keine Anlasslosigkeit, wenn Maßnahmen Verdächtige oder Verurteilte betreffen; jedenfalls spricht er zunächst von der Verwendung von Daten von „ehemals Verdächtigen oder Verurteilten" und dann davon, dass ein „sehr viel strengerer Maßstab […] *hingegen* jedenfalls für Personen gelten [muss], die keinen zurechenbaren Anlass für eine Erfassung ihrer Daten gesetzt haben" (*Singelnstein*, NStZ 2018, 1, 6; Hervorhebung J. H.).

393 Vereinzelt scheinen Polizeibehörden auch bei dem Verdacht einer Ordnungswidrigkeit auf § 81b Alt. 2 StPO zurückzugreifen; hierzu kritisch *Der Bayerische Landesbeauftragte für den Datenschutz*, Tätigkeitsbericht 2021, 31 f.

Voraussetzungen hierfür vorlagen.[394] Mehr noch: Für eine Anordnung der Maßnahmen „für die Zwecke des Erkennungsdienstes" (§ 81b Alt. 2 StPO) ist es ausreichend, wenn mit Blick auf die Anlasstat „Verdachtsmomente" gegen den Betroffenen bestehen.[395] Diese entsprechen dem Anfangsverdacht nach § 152 Abs. 2 StPO und können als „Restverdacht" selbst dann fortbestehen, wenn das Verfahren eingestellt wurde[396] und sogar dann, wenn der Betroffene rechtskräftig freigesprochen wurde[397].[398] Es erschließt sich nicht, inwiefern eine Person, die irgendwann einmal wegen einer Straftat *verdächtigt* wurde, einen Anlass dafür gibt, zum Abgleich mit dem Täter jeder beliebigen irgendwo in Deutschland begangenen Straftat herangezogen zu werden, die per Gesichtserkennung aufgeklärt werden soll.

Der Umstand, dass gegenüber diesen Personen erkennungsdienstliche Maßnahmen nach § 81b Alt. 2 StPO angeordnet, also insbesondere auch Lichtbilder von ihnen angefertigt und gespeichert werden durften, ändert daran nichts.[399] Zwar ließe sich argumentieren, dass die Vorschrift des § 81b Alt. 2 StPO zum Ausdruck bringt, dass ein Anlass besteht, das Lichtbild des Betroffenen grundsätzlich in Zukunft erneut zu verwenden. Dies geht aber automatisch mit einem Filter einher. Die Polizeibeamten würden bereits aus Ressourcengründen nicht beliebig alle ihnen zugänglichen Lichtbilder

394 Bei Alt. 2 muss also insbesondere eine Notwendigkeit der erkennungsdienstlichen Behandlung für die Aufklärung künftiger Straftaten bestehen (Wiederholungsgefahr), hierzu näher etwa MüKoStPO/*Trück*, 2. Aufl. 2023, StPO § 81b Rn. 10 ff.

395 Siehe nur OVG Greifswald, Urt. v. 25.11.2015, 3 L 146/13, BeckRS 2016, 42877 Rn. 43, 45 ff.; VGH Mannheim, Urt. v. 13.7.2011, 1 S 350/11, BeckRS 2011, 53016; OVG Lüneburg, Beschl. v. 31.8.2010, 11 ME 288/10, StV 2010, 676, 677; VGH Kassel, Urt. v. 16.12.2004, 11 UE 2982/02, NJW 2005, 2727, 2729, 2731.

396 Siehe etwa OVG Bautzen, Urt. v. 19.4.2018, 3 A 215/17, BeckRS 2018, 7292 Rn. 22; OVG Münster, Beschl. v. 14.4.2010, 5 A 479/09, BeckRS 2010, 49130.

397 BVerfG, NJW 2002, 3231. Vgl. auch BayVGH, Beschl. v. 24.2.2015 – 10 C 14.1180; BayVGH, Beschl. v. 21.10.2002 - 24 C 02.2268.

398 Denn die Speicherung erfolgt zu präventiv-polizeilichen Zwecken, vgl. nur BVerfG, NJW 2002, 3231, 3232. Zum Ganzen mwN auch BeckOK StPO/*Goers*, 49. Ed., Stand: 1.10.2023, StPO § 81b Rn. 7 und MüKoStPO/*Trück*, 2. Aufl. 2023, StPO § 81b Rn. 11.

399 Anders wohl *Schindler*, Biometrische Videoüberwachung, 2021, 509 Fn. 2579, wonach zwar „argumentiert werden könnte, dass bei jedem Abgleich alle in der Datenbank erfassten Personen in den Abgleich einbezogen werden, so dass insoweit zahlreiche Personen betroffen sind. Allerdings handelt es sich bei Personen in erkennungsdienstlichen Datenbanken nicht um ‚unbescholtene' Bürger, die keinerlei Anlass für eine Maßnahme gegeben haben, sondern um Personen, deren Lichtbilder aufgrund besonderer Befugnisse angefertigt (z. B. § 81b StPO) und gespeichert wurden."

jeder Person bei jedem Delikt durchblättern, sondern anhand von Anhaltspunkten entscheiden, welche Personen näher betrachtet werden. Dieser Filter fällt bei einer automatisierten Suche per Gesichtserkennung weg, denn hiermit kann in Sekundenschnelle eine große Datenbank mit Millionen Fotos durchsucht werden. Einen Anlass für eine erkennungsdienstliche Behandlung zu geben, bedeutet nicht, einen Anlass für einen Abgleich mit dem Täter einer beliebigen irgendwo in Deutschland begangenen Straftat zu geben, dessen Identität per Gesichtserkennung ermittelt werden soll.

Zudem erscheint es eine Überlegung wert, bei der (normativen) Bestimmung, ob eine Person zurechenbar Anlass zum Gesichtserkennungsabgleich gegeben hat, wertend Aspekte der Rechtswirklichkeit zu berücksichtigen. Denn bereits mit Blick auf die ursprüngliche erkennungsdienstliche Behandlung kann in rechtstatsächlicher Hinsicht durchaus in Frage gestellt werden, ob jeder, der einer solchen unterzogen wurde, hierzu überhaupt *durch sein Verhalten* einen Anlass gegeben hat. Voraussetzung für eine Maßnahme nach § 81b StPO sind insbesondere „Verdachtsmomente".[400] Sowohl mit Blick auf die Sachverhaltsfeststellung und -beurteilung als auch die „kriminalistische Erfahrung", anhand derer zureichende Anhaltspunkte für einen Anfangsverdacht begründet werden, besteht ein erheblicher Spielraum, der Einfallstor auch für Diskriminierung sein kann.[401] Vorurteile gegen Angehörige bestimmter Bevölkerungsgruppen können dazu führen,

400 MüKoStPO/*Trück*, 2. Aufl. 2023, StPO § 81b Rn. 11; BVerfG, NJW 2002, 3231.

401 *Walburg*, in: Hunold/Singelnstein Rassismus in der Polizei, 2022, 385, 393 f., insbesondere S. 393: „Ob […] bei einer oft noch mehrdeutigen Beobachtung mit häufig unvollständigen Informationen, aber auch bei der Entgegennahme einer Strafanzeige, ein Verdacht angenommen wird, und inwiefern sowie mit wieviel Elan dieser weiterverfolgt wird, ist von verschiedenen Faktoren abhängig. Neben gegebenenfalls konfligierenden Aufgaben und begrenzten Ressourcen kommen bei der Sachverhaltsfeststellung und -beurteilung, bei der die zwischen Devianten und Angepassten unterscheidende soziale Ordnung hergestellt wird […], abermals tradierte Situationsdeutungen, zugrundeliegende Wissensbestände sowie Handlungsroutinen ins Spiel. Auch diese Entscheidungen sind daher ein mögliches Einfallstor für Stereotype und darauf gestützte diskriminierende Praktiken."; *Ricker*, Anfangsverdacht und Vorurteil, 2021, 167, 181 ff. Vgl. zudem dazu, dass Personen einiger Bevölkerungsgruppen häufiger polizeilich kontrolliert werden nur erneut *Niemz/Singelnstein*, in: Hunold/Singelnstein, Rassismus in der Polizei, 2022, 337; *Abdul-Rahman*, in: Hunold/Singelnstein Rassismus in der Polizei, 2022, 471, 479 mwN; *Hunold/Wegner*, Aus Politik und Zeitgeschichte 2020, 27, 30 f.; *Hunold*, Polizei im Revier, 2015, 103 ff.; *Schweer/Strasser/Zdun*, „Das da draußen ist ein Zoo, und wir sind die Dompteure" – Polizisten im Konflikt mit ethnischen Minderheiten und sozialen Randgruppen, 2008; *Schweer/Strasser*, in: Groenemeyer/Mansel, Die Ethnisierung von Alltagskonflikten, 2003, 229.

dass bei ihnen vorschnell ein Verdacht bejaht wird[402] und sie daher mitunter auch vorschnell observiert, kontrolliert, durchsucht, festgenommen und erkennungsdienstlich behandelt werden[403]. Es ist zweifelhaft, ob diese Personen hierfür tatsächlich immer „durch ihr Verhalten" einen Anlass gegeben haben (womöglich mitunter eher: durch ihr Erscheinungsbild).

Im Übrigen sei daran erinnert, dass die Annahme einer Anlasslosigkeit nicht bedeutet, dass ein Gesichtserkennungsabgleich mit diesen Personen per se unzulässig ist. Die Konsequenz ist aber, dass hieran strenge Anforderungen zu stellen sind, da durch die Einbeziehung vieler Personen, die hierzu keinen Anlass gegeben haben, eine große Streubreite und damit ein erhebliches Eingriffsgewicht der Maßnahme besteht.

Jedenfalls aber geben Asylsuchende nicht generell Anlass dazu, in einen Gesichtserkennungsabgleich zur Ermittlung der Identität unbekannter Straftatverdächtiger einbezogen zu werden. Auch wenn die Lichtbilder der Asylsuchenden separat von denen Verurteilte und Verdächtiger gespeichert sind: Indem alle Asylsuchenden pauschal bei jeder Gesichtserkennungssuche dahingehend überprüft werden, ob sie der Täter waren, stellt man sie faktisch unter einen Generalverdacht. Allein mit Blick auf sie wird deutlich, dass die Gesichtserkennungsrecherchen eine Vielzahl von Personen erfassen, die hierzu keinerlei Anlass gegeben haben. Dies erhöht die Eingriffsintensität beträchtlich.

cc) Einschüchterungseffekte

Das Bundesverfassungsgericht argumentiert im Zusammenhang mit der Streubreite und Anlasslosigkeit von Maßnahmen zudem häufig mit Einschüchterungseffekten.[404] Diese könnten zu Beeinträchtigungen bei der Ausübung von Grundrechten führen.[405] Hierdurch werde auch das Ge-

402 *Ricker*, Anfangsverdacht und Vorurteil, 2021, 121 f.

403 *Feuerhelm*, Polizei und „Zigeuner", 1987, 184, 194 f., 208 f., 234.

404 Vgl. nur BVerfGE 113, 29 (46); 115, 320 (354); 120, 378 (402); 156, 11 (54). *Kube* spricht etwa davon, dass sich gerade „auf der Nutzung der Informationstechnologie beruhende, lautlose und punktuelle Beeinträchtigungen aus der Distanz als besonders eingriffsintensiv darstellen können, weil der Staat dem Bürger hier nicht rechtsstaatlich offen und greifbar entgegentritt, sondern im verborgenen [sic!] bleibt und potentiell omnipräsent ist.", *Kube*, in: Isensee/Kirchhof, Handbuch des Staatsrechts, Band VII, 3. Aufl. 2009, § 148 Rn. 81.

405 Vgl. nur BVerfGE 65, 1 (42); 113, 29 (46).

meinwohl beeinträchtigt, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger gegründeten freiheitlichen demokratischen Gemeinwesens sei.[406] Es gefährde die Unbefangenheit des Verhaltens, wenn die Streubreite von Ermittlungsmaßnahmen dazu beitrage, dass Risiken des Missbrauchs und ein Gefühl des Überwachtwerdens entstünden.[407] Wenig konkret führt das Bundesverfassungsgericht dies zurück auf ein „Gefühl des unkontrollierbaren Beobachtetwerdens"[408], ein „diffus bedrohliches Gefühl des Beobachtetseins"[409] oder eine „diffuse Bedrohlichkeit"[410].[411]

Zwar wird der Rückgriff auf Einschüchterungseffekte – nicht zuletzt wegen fehlender Empirie[412] – zu Recht vielfach kritisiert. Das Bundesverfassungsgericht greift auf diese Argumentationsfigur aber jedenfalls zurück, sodass sie auch mit Blick auf die Gesichtserkennung eine Rolle spielen kann. Beim Einsatz zur Identifizierung unbekannter Verdächtiger durch Recherche in einer Lichtbilddatenbank ließe sich argumentieren, dass die Verwendung von Gesichtserkennung dazu führe, dass jeder, der in der durchsuchten Datenbank gespeichert ist, ständig damit rechnen müsse, mit unbekannten Verdächtigen abgeglichen zu werden und zudem Sorge davor haben müsse, womöglich zu Unrecht identifiziert zu werden, sodass dann

406 BVerfGE 115, 320 (354), vgl. auch BVerfGE 113, 29 (46).
407 BVerfGE 107, 299 (328); 115, 320 (354).
408 BVerfGE 125, 260 (332); 156, 11 (54).
409 BVerfGE 120, 378 (402); 125, 260 (320).
410 BVerfGE 150, 244 (268, 283).
411 Überzeugender hingegen die Formulierung bei *Poscher/Buchheim*, DVBl 2015, 1273, 1279, dass eine Grundrechtsgefährdung „plausibilisiert" werden muss (die hierin bereits einen Eingriff in das Recht auf informationelle Selbstbestimmung sehen). Zur Rekonstruktion des Rechts auf informationelle Selbstbestimmung als Schutz vor Grundrechtsgefährdungen *Poscher*, in: Gander/Perron/Poscher/Riescher/Würtenberger, Resilienz in der offenen Gesellschaft, 2012, 167; vgl. in eine ähnliche Richtung *Britz*, in: Hoffmann-Riem, Offene Rechtswissenschaft, 2010, 561, 569 ff.
412 Sondervotum Eichberger, BVerfGE 125, 260 (380 ff., Rn. 337 ff.; 381, Rn. 338); *Staben*, Der Abschreckungseffekt auf die Grundrechtsausübung, 2016, 121 ff., (speziell auch zur fehlenden Empirie für Deutschland); kritisch auch *Bull*, Informationelle Selbstbestimmung – Vision oder Illusion?, 2. Aufl. 2011, 63 f., 97 ff.; *Nettesheim*, VVDStRL 2011, 7, 28; zur fehlenden Empirie siehe auch *Sklansky*, California Law Review 2014, 1069, 1094 ff.; *De Mot/Faure*, Tort Law Review 2014, 120, 121. Zu weiteren Kritikpunkten siehe etwa *Schwabenbauer*, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, Kapitel G. Informationsverarbeitung im Polizei- und Strafverfahrensrecht, Rn. 134 (Unvereinbarkeit mit der Ausrichtung der Eingriffsdogmatik am individuellen Freiheitsschutz), siehe auch Dreier GG/*Barczak*, 4. Aufl. 2023, GG Art. 2 Abs. 1 Rn. 101.

ohne sein Wissen noch weitere Ermittlungen über ihn geführt werden. Ob zudem die Auswertung von Aufzeichnungen potenzieller Tatverdächtiger bei einer Versammlung zu Einschüchterungseffekten führt, wird im Abschnitt zur Versammlungsfreiheit betrachtet.[413]

dd) Anknüpfen an höchstpersönliche Merkmale

Erschwerend tritt hinzu, dass Gesichtserkennung an das Gesicht und damit an höchstpersönliche Merkmale anknüpft.[414] In der Entscheidung zu automatisierten Kfz-Kennzeichenkontrollen berücksichtigte das Bundesverfassungsgericht ausdrücklich mildernd, dass die Maßnahme gerade *nicht* „an höchstpersönliche Merkmale wie etwa das Gesicht anknüpft, sondern an öffentliche Kennzeichen, die nur mittelbar auf einige begrenzte Halterdaten hinweisen".[415] Der Personenbezug lasse sich nur mittelbar herstellen.[416]

Dagegen wird bei der Gesichtserkennung direkt an ein höchstpersönliches körperliches Merkmal angeknüpft.[417] Zudem handelt es sich bei den extrahierten Gesichtsmerkmalen um biometrische Merkmale[418], die sekundärrechtlich (vgl. Art. 9 Abs. 1, 2 DSGVO sowie Art. 10 JI-RL) besonders geschützt sind und auch auf Ebene des Verfassungsrechts eine besondere Beachtung verdienen.[419] Das Bundesverfassungsgericht scheint die beson-

413 Kapitel II. A. II.

414 Vgl. auch *Schwabenbauer*, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, Kapitel G. Informationsverarbeitung im Polizei- und Strafverfahrensrecht, Rn. 121, *Schindler*, Biometrische Videoüberwachung, 2021, 485; *Stettner*, Sicherheit am Bahnhof, 2017, 150. Siehe zudem BVerfGE 150, 244 (269) („Bedeutsam ist dabei auch, dass […] nur Ort, Datum, Uhrzeit und Fahrtrichtung erfasst werden, nicht aber die Personen oder die Kraftfahrzeuge."). Vgl. zur Bedeutung der Sensibilität der Daten für die Intensität des Eingriffs auch *Heckmann/Paschke*, in: Stern/Sodan/Möstl, Das Staatsrecht der Bundesrepublik Deutschland im europäischen Staatenverbund, 2. Aufl. 2022, § 103 Datenschutz, Rn. 45.

415 BVerfGE 150, 244 (269).

416 BVerfGE 150, 244 (283).

417 Vgl. auch *Kulick*, NVwZ 2020, 1622, 1625.

418 Vgl. erneut die Definition in Art. 3 Nr. 13 JI-RL und Art. 3 Nr. 34 KI-VO: Biometrische Daten sind „mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen".

419 In diese Richtung auch *Martini/Thiessen/Ganter*, Digitale Versammlungsbeobachtung, 2023, 62 f.

dere Schutzwürdigkeit biometrischer Merkmale ebenfalls anzuerkennen, wenn es den Ausschluss biometrischer Merkmale bei einer Datenanalyse als eingriffsmildernd ansieht.[420] Beim Gesicht handelt es sich zudem um ein biometrisches Merkmal, das nicht etwa verhaltensbezogen (dynamisch) ist wie etwa die Stimme, die Unterschrift oder der Anschlagsrhythmus der Tastatur, sondern physisch: Es ist angeboren, weitgehend unveränderlich und kann – anders als ein Autokennzeichen – nicht gewechselt oder zu Hause gelassen werden.[421] Damit geht auch einher, dass die durch Gesichtserkennung gewonnenen Informationen eine besondere Persönlichkeitsrelevanz aufweisen können. Dem Gesicht kommt auch eine herausgehobene Bedeutung zu, da es zudem noch (anders als etwa Fingerabdrücke) aus einer gewissen Distanz leicht erkennbar und auf Fotos oder Videos leicht heimlich erfassbar ist.

ee) Möglichkeit der Verknüpfung von Informationen

Eng mit der Persönlichkeitsrelevanz verbunden ist die Möglichkeit der Verknüpfung von Informationen sowie der Profilbildung, die ebenfalls die Eingriffsintensität erhöhen.[422] Dabei kommt es gerade nicht darauf an, ob die Informationen *tatsächlich* verknüpft oder Persönlichkeits- und Bewegungsprofile erstellt werden. Entscheidend ist vielmehr, dass dies durch die Maßnahme *möglich* wäre.[423] Denn das Recht auf informationelle Selbstbestimmung will auch Gefährdungen im Vorfeld der Bedrohung konkreter

420 BVerfGE 165, 363 (404).

421 Auch wenn bei der Identifizierung unbekannter Verdächtiger Gesichtserkennung nur punktuell eingesetzt wird; potenziell lässt ihr Einsatz tief in das Leben des Betroffenen blicken. Wenn etwa verschiedene Videoaufzeichnungen einer Person per Gesichtserkennung kombiniert werden, kann herausgefunden werden, wo er sich aufgehalten und mit wem er interagiert hat.

422 Zur Unzulässigkeit der Erstellung von umfassenden Persönlichkeitsprofilen bereits BVerfGE 65, 1 (53); vgl. zudem zuvor schon BVerfGE 27, 1 (6).

423 Siehe etwa BVerfGE 125, 260 (292): „Umfassende Persönlichkeitsprofile *könnten* erstellt werden." (Hervorhebung J. H.) und BVerfGE 125, 260 (319): „Je nach Nutzung der Telekommunikation und künftig in zunehmender Dichte *kann* eine solche Speicherung die Erstellung aussagekräftiger Persönlichkeits- und Bewegungsprofile praktisch jeden Bürgers *ermöglichen*." (Hervorhebung J. H.). Kritisch zu solchen Befürchtungen etwa *Trute*, Die Verwaltung 2009, 85, 100 f.; *Zöller*, Informationssysteme und Vorfeldmaßnahmen von Polizei, Staatsanwaltschaft und Nachrichtendiensten, 2002, 43.

Rechtsgüter verhindern.[424] Eingriffserhöhend wirken daher auch bereits Missbrauchsmöglichkeiten, die mit einer Datensammlung einhergehen;[425] im Rahmen der Rechtfertigung einer solchen Maßnahme ist daher auch zu prüfen, ob Sicherungen gegen einen Missbrauch der Daten bestehen.

Gesichtserkennung macht es besonders leicht, unterschiedlichste Informationen über eine Person zu verknüpfen, da etwa alle Video- und Fotoaufnahmen einer Person, die in staatlicher Hand sind, zusammengeführt werden könnten. Zwar ist dies im konkreten Einsatzszenario der Verwendung von Gesichtserkennung zur Identifizierung von unbekannten Verdächtigen nicht das Ziel. Gerade wenn eine Person aber beispielsweise mehrmals stiehlt, kann es vorkommen, dass (zufällig) mehrmals Aufnahme derselben Person eingereicht werden; die daraus gewonnen Informationen können verknüpft werden. Auch in Anbetracht dessen, dass der Einsatz von Gesichtserkennung – und damit auch die Grenzen – gar nicht ausdrücklich in der Strafprozessordnung geregelt sind und zugleich jeden Tag nicht bewältigbare große Mengen staatlicher Videoaufnahmen generiert werden (die ausgewertet werden wollen), erscheint es angezeigt, bereits die abstrakte Gefahr der leichten Verknüpfbarkeit von Informationen durch Gesichtserkennung eingriffserhöhend zu berücksichtigen.

ff) Drohende Nachteile

Weiter hängt das Eingriffsgewicht davon ab, welche Nachteile einem Grundrechtsträger aufgrund der Maßnahme darüber hinaus drohen oder

424 Vgl. nur BVerfGE 150, 244 (264); vgl. auch *Bäcker*, Der Staat 2012, 91, 94 ff. und die Konzeption des Rechts auf informationelle Selbstbestimmung bei *Poscher*, in: Gander/Perron/Poscher/Riescher/Würtenberger, Resilienz in der offenen Gesellschaft, 2012, 167, 174 ff.

425 Siehe etwa BVerfGE 125, 260 (320): „Auch die Missbrauchsmöglichkeiten, die mit einer solchen Datensammlung verbunden sind, verschärfen deren belastende Wirkung.“. *Heckmann/Paschke*, in: Stern/Sodan/Möstl, Das Staatsrecht der Bundesrepublik Deutschland im europäischen Staatenverbund, 2. Aufl. 2022, § 103 Datenschutz, Rn. 45; treffend im Übrigen mit Blick auf Erbgutanalysen Dürig/Herzog/Scholz/*Di Fabio*, 102. EL August 2023, GG Art. 2 Abs. 1 Rn. 159 Fn. 17 („Das eigentliche Eingriffspotential von Erbgutanalysen liegt nicht im bestimmungsgemäßen Gebrauch, hier unterscheiden sie sich kaum vom Fingerabdruck, sondern in Missbrauchsmöglichkeiten hinsichtlich der damit gewonnenen, über den Aufklärungszweck hinausreichenden, Erbgutinformationen.“).

von ihm nicht ohne Grund befürchtet werden.[426] In der Entscheidung zur Rasterfahndung führte das Bundesverfassungsgericht etwa aus, dass „die Übermittlung und Verwendung von Daten für die davon Betroffenen das Risiko begründen [könne], Gegenstand staatlicher Ermittlungsmaßnahmen zu werden, das über das allgemeine Risiko hinausgeht, einem unberechtigten Verdacht ausgesetzt zu werden".[427]

Ebenso verhält es sich bei der automatisierten Gesichtserkennung. Sie dient gerade dazu, einen Verdacht (gegen Unbekannt) zu einem Verdacht gegen eine (nun namentlich benennbare) Person zu konkretisieren und in der Folge durch weitere Ermittlungsmaßnahmen gegen diese Person herauszufinden, ob sie etwa auch in der Nähe des Tatorts war oder andere Verbindungen zum Tatgeschehen hat. Daher geht der Eingriff „Abgleich per Gesichtserkennung" womöglich mit weiteren intensiven Grundrechtseingriffen einher; erst recht besteht diese Gefahr für diejenigen, die auf der Trefferliste auftauchen.[428] Wie bei der Rasterfahndung besteht auch bei der Identifizierung nach einer Gesichtserkennungsrecherche die Gefahr, unberechtigt staatlichen Ermittlungsmaßnahmen ausgesetzt zu sein.[429]

Welches Gewicht diesen möglichen nachteiligen Wirkungen einer informationsbezogenen Maßnahme im Hinblick auf die Beurteilung dieser Maßnahme zukommt, soll nach der Rechtsprechung auch davon abhängen, welche Möglichkeit der Grundrechtsträger hat, eine eventuelle Grundrechtsbeeinträchtigung oder jedenfalls weitere Folgen des Eingriffs abwehren zu können.[430] Bei heimlichen Maßnahmen wie der automatisierten Gesichtserkennung kann zumindest diese Maßnahme als solche nicht abgewehrt werden; auch die Folgeeingriffe (weitere Ermittlungsmaßnahmen) sind als strafprozessuale Maßnahmen schwerlich abwendbar.

426 Vgl. BVerfGE 100, 313 (376); 113, 348 (382); 115, 320 (347); 118, 168 (197).

427 BVerfGE 115, 320 (351); vgl. auch BVerfGE 107, 299 (321); 118, 168 (197). Auch könnten informationsbezogene Ermittlungsmaßnahmen „im Falle ihres Bekanntwerdens eine stigmatisierende Wirkung für die Betroffenen haben und so mittelbar das Risiko erhöhen, im Alltag oder im Berufsleben diskriminiert zu werden".

428 Vgl. auch *Schindler*, Biometrische Videoüberwachung, 2021, 509 f.

429 Wie bereits angesprochen, ist beim Einsatz von Gesichtserkennung die Gefahr sogar erhöht, dass Unbeteiligte in den Fokus der Polizei geraten und dass dies wegen einer starken optischen Ähnlichkeit nicht frühzeitig entdeckt wird, siehe hierzu bereits Kapitel I. D. I. 2.

430 Vgl. BVerfGE 118, 168 (197).

gg) Eigener Ansatz zur Fortschreibung der Maßstäbe: Spezifische Fehleranfälligkeit der Maßnahme

Zudem erscheint es eine Überlegung wert, die spezifische Fehleranfälligkeit einer Maßnahme als eigenständiges Kriterium beim Eingriffsgewicht heranzuziehen. In seiner Entscheidung zur automatisierten Datenanalyse deutet das Bundesverfassungsgericht zumindest kurz an, dass die Frage, „wie fehleranfällig die eingesetzte Datenauswertungstechnologie ist und ob gegebenenfalls Vorkehrungen zur Entdeckung und Korrektur von Fehlern getroffen sind" die Eingriffsintensität einer Datenanalysemaßnahme beeinflussen.[431] Das Gericht berücksichtigt außerdem das Risiko, dass Personen einem unberechtigten Verdacht ausgesetzt werden, teilweise bei den Kriterien Streubreite/Anlasslosigkeit[432] und mögliche Folgeeingriffe nach einer Maßnahme[433]. Denn durch die Verarbeitung von Daten Unverdächtiger werde das Risiko geschaffen, einem unberechtigten Verdacht ausgesetzt zu werden.[434] In der Entscheidung zu automatisierten Kfz-Kennzeichenkontrollen[435] äußert sich das Gericht allerdings gar nicht zu den „unechten" (also falschen) Treffern, obwohl es feststellt, dass von den etwa 40.000 bis 50.000 Treffermeldungen, die in einem Zeitraum von vier Monaten

431 BVerfGE 165, 363 (409).

432 Siehe z. B. BVerfGE 107, 299 (321): „Wird die Kommunikation Unverdächtiger erfasst, so schafft die Erhebung der Verbindungsdaten für sie das Risiko, Gegenstand staatlicher Ermittlungen zu sein, das zu dem allgemeinen Risiko hinzutritt, einem unberechtigten Verdacht ausgesetzt zu werden."; ähnlich auch *Bäcker*, in: Herdegen/Masing/Poscher/Gärditz, Handbuch des Verfassungsrechts, 2021, § 28 Sicherheitsverfassungsrecht, Rn. 92, wonach sich aus der großen Streubreite „ein gesteigertes Risiko [ergebe], dass solche Personen aufgrund eines falsch positiven sicherheitsbehördlichen Wahrscheinlichkeitsurteils weiteren Eingriffsmaßnahmen ausgesetzt werden.", dazu auch bereits *Bäcker*, Kriminalpräventionsrecht, 2015, 270 ff.; *Schwabenbauer*, Grundrechtseingriffe, 2013, 167 ff.

433 Siehe z. B. BVerfGE 115, 320 (351): „Das Gewicht informationsbezogener Grundrechtseingriffe richtet sich auch danach, welche Nachteile den Betroffenen aufgrund der Eingriffe drohen oder von ihnen nicht ohne Grund befürchtet werden […]. So kann die Übermittlung und Verwendung von Daten für die davon Betroffenen das Risiko begründen, Gegenstand staatlicher Ermittlungsmaßnahmen zu werden, das über das allgemeine Risiko hinausgeht, einem unberechtigten Verdacht ausgesetzt zu werden […]."

434 Vgl. BVerfGE 107, 299 (321); 115, 320 (351); 125, 260 (320).

435 BVerfGE 150, 244.

generiert wurden, nur 500 bis 600 echte Treffer waren.[436] Der Grund dafür könnte darin liegen, dass bei falschen Treffern bei der Kfz-Kennzeichenkontrolle Folgemaßnahmen gegen Unschuldige sehr unwahrscheinlich sind, da Fehler sehr leicht erkennbar sind: das als Treffer gemeldete Kennzeichen befindet sich nicht auf der Fahndungsliste. Dies kann durch einen einfachen Vergleich der Ziffern und Buchstaben der Kennzeichen überprüft werden. „Grauzonen" wie beim Vergleich zweier Gesichter und damit eine besondere Fehleranfälligkeit gibt es insofern nicht.[437] In der Entscheidung zur Vorratsdatenspeicherung aus dem Jahr 2010 beispielsweise berücksichtigte das Gericht hingegen ausdrücklich den Umstand, dass das „Risiko von Bürgern erheblich steigt, weiteren Ermittlungen ausgesetzt zu werden, ohne selbst Anlass dazu gegeben zu haben".[438] Denn es könne etwa ausreichen, „zu einem ungünstigen Zeitpunkt in einer bestimmten Funkzelle gewesen oder von einer bestimmten Person kontaktiert worden zu sein, um in weitem Umfang Ermittlungen ausgesetzt zu werden und unter Erklärungsdruck zu geraten".[439]

Wie mit Blick auf die automatisierte Gesichtserkennung deutlich wird, könnte es aber sinnvoll sein, die spezifische Fehleranfälligkeit einer Maßnahme als eigenständiges Kriterium zu betrachten. Das gilt erst recht, wenn eine Technologie im Verdacht steht, bei einzelnen Bevölkerungsgruppen sogar noch mehr Fehler zu machen.[440] Bei der Gesichtserkennung beruht die Gefahr, unberechtigt verdächtigt zu werden, nicht lediglich auf der Streubreite, sondern ist aufgrund der Funktionsweise dieser Technologie

436 Auch in der ersten Entscheidung zur automatisierten Erfassung von Kfz-Kennzeichen differenziert das Bundesverfassungsgericht gar nicht zwischen echten und unechten Treffern, vgl. BVerfGE 120, 378.

437 Zu Problemen bei der Überprüfung kann es nur kommen, wenn das aufgezeichnete Kennzeichen (z. B. wegen Verschmutzung oder schlechter Wetterverhältnisse) schwer zu erkennen ist.

438 BVerfGE 125, 260 (320).

439 BVerfGE 125, 260 (320).

440 In diese Richtung deutet BVerfGE 165, 363 (408) („Eine spezifische Herausforderung [des Einsatzes Künstlicher Intelligenz] besteht darüber hinaus darin, die Herausbildung und Verwendung diskriminierender Algorithmen zu verhindern. "). Angesichts des aktuellen Stands der Technik mit Blick auf unterschiedliche Fehlerraten für unterschiedliche Bevölkerungsgruppen (Kapitel I. E. IV. 5.) muss gerade für Gesichtserkennungssysteme wie das GES, die offenbar nicht selbst evaluiert werden (weder allgemein noch mit Blick auf verschiedene Bevölkerungsgruppen), der *Verdacht* ausreichen, dass auch dieses System höhere Fehlerraten für einzelne Bevölkerungsgruppen aufweist und insofern „verzerrt" sein könnte.

noch spezifisch erhöht:[441] Es sollen gerade möglichst ähnliche Gesichter zum unbekannten Verdächtigen gefunden werden. Die nun ins Visier genommene Person war nicht nur zu einem ungünstigen Zeitpunkt in einer bestimmten Funkzelle oder von einer bestimmten Person kontaktiert worden, sondern sie sieht aus wie der Verdächtige.

Diese Fehleranfälligkeit kann auch nicht vollständig durch die menschliche Kontrolle der Gesichtserkennungstreffer abgefangen werden. Denn auch diese ist nicht fehlerfrei.[442] Insbesondere können die Lichtbildexperten oder -sachverständigen aus der Liste die falsche Person auswählen (zumal nach geltendem Recht nicht eindeutig vorgeschrieben ist, dass und wie die identifizierende Person geschult sein muss). Wenn das Bild des unbekannten Verdächtigen von hoher Qualität ist, dann ist dies zwar wenig wahrscheinlich (allerdings dennoch möglich). Falsch liegen können die Experten – und erst recht nicht geschulte Polizeibeamte – aber gerade in den Fällen, in denen das Bild nicht von ausreichender Qualität ist, um einen detaillierten (menschlichen) Abgleich durchzuführen und daher lediglich ein Verdacht der Personenidentität als ermittlungsunterstützender Hinweis besteht.[443] Damit ist nicht gemeint, dass ihnen der Fehler *vorwerfbar* ist, denn sie legen schließlich offen, dass eine nähere Aussage nicht möglich ist. Dennoch können die Polizisten mit diesem Verdacht einer Personenidentität weiterermitteln, um herauszufinden, ob andere Hinweise darauf hindeuten, dass es sich bei dem Identifizierten um den gesuchten Täter handelt. Auch wenn die Ermittlungsbeamten dann dieser Person im realen Leben gegenüberstehen, klärt sich nicht direkt auf, wenn der Verdacht auf einen Unschuldigen gefallen ist. Denn sie haben zum (menschlichen) Abgleich dieser nun realen Person weiterhin nur das Bild des unbekannten Verdächtigen mit schlechter Qualität.[444] Automatisierte Gesichtserkennung geht

441 Siehe Kapitel I. D. I. 2. Anders *Schindler*, Biometrische Videoüberwachung, 2021, 510 („Fehlerhafte Erkennungen sind auch bei der anlassbezogenen Suche in Lichtbilddatenbanken nicht auszuschließen. Da der Gesichtserkennung hier aber letzten Endes nur eine Filter- und Sortierfunktion zukommt, ist von vornherein eine menschliche Überprüfung der Ergebnisse vorgesehen. Die eigentliche Zuordnung erfolgt somit durch menschliche Spezialisten. […] Diese können zwar ebenfalls Fehler machen. Dabei realisiert sich dann aber kein spezifisches Risiko der Gesichtserkennung.“).

442 Zu den in der Verantwortung von Menschen liegenden Fehlern im Zusammenhang mit Gesichtserkennung vertieft Kapitel III. B. II. 2. und 3.

443 Kapitel I. F. I. 2. c).

444 Zudem sind sie weniger geschult als die Experten, eine Personenidentität zu erkennen.

daher mit der spezifisch erhöhten Gefahr einher, dass gegen Unschuldige ermittelt wird *und dass dies nicht frühzeitig erkannt wird*. Diese spezifische Fehleranfälligkeit könnte als eigenes Kriterium für ein erhöhtes Eingriffsgewicht bei der automatisierten Gesichtserkennung berücksichtigt und in Zukunft auch für andere datenbasierte polizeiliche Maßnahmen untersucht werden.

hh) Eingriffsgewicht mindernde Umstände

Andererseits sind auch Umstände zu berücksichtigen, die das Eingriffsgewicht reduzieren. So wirkt sich mindernd aus, dass in den Gesichtserkennungsvorgang zwar Daten vieler überwiegend nicht beteiligter Personen einbezogen werden, der Datenabgleich aber in Sekundenschnelle durchgeführt wird und die erfassten Daten im Nichttrefferfall keine weitere polizeiliche Tätigkeit veranlassen.[445] Weiter reduziert es die Eingriffsintensität, dass zumindest die den Embeddings zugrunde liegenden Lichtbilder nicht erst für die Gesichtserkennung erhoben wurden, sondern die Strafverfolgungsbehörden die Daten bereits gesetzlich legitimiert erhoben haben.[446]

Nicht eingriffsmindernd wirkt sich hingegen aus, dass ein konkreter Anlass für den Abgleich besteht (Begehung einer Straftat und Notwendigkeit der Identifizierung des Verdächtigen).[447] Denn es ist gerade der Regelfall, dass ein Anlass für eine Datenverarbeitung bestehen muss; nur wenn sie ausnahmsweise anlasslos erfolgt, ist der Eingriff umgekehrt besonders intensiv.[448]

---

445 Vgl. BVerfGE 165, 36 (403 f.) zur automatisierten Datenanalyse; vgl. auch zur automatisierten Kfz-Kennzeichenkontrolle BVerfGE 150, 244 (283).

446 In diese Richtung wohl auch *Schindler*, Biometrische Videoüberwachung, 2021, 510 („bereits aufgrund anderer Maßnahmen (z. B. Videoüberwachung oder erkennungsdienstlicher Behandlung) im Besitz der polizeilichen Stellen"); *Hornung/Schindler*, ZD 2017, 203, 207 („bereits auf Grundlage anderer gesetzlicher Ermächtigungen in der Verfügungsgewalt der staatlichen Behörden"); *Petri*, GSZ 2018, 144, 148. („bereits erhobener Bilddaten"). Dies ändert jedoch, wie oben angesprochen, nichts daran, dass diese Personen keinen Anlass für den Abgleich gegeben haben, vgl. Kapitel II. A. I. 2. b) bb).

447 In diese Richtung aber offenbar *Hornung/Schindler*, ZD 2017, 203, 207, die ein „vergleichsweise geringe[s][…] Eingriffsgewicht" annehmen, da im Rahmen eines „Strafverfahrens *aus konkretem Anlass* nur Daten miteinander abgeglichen [werden], die sich bereits auf Grundlage anderer gesetzlicher Ermächtigungen in der Verfügungsgewalt der staatlichen Behörden befinden" (Hervorhebung J. H.).

448 Vgl. etwa BVerfGE 125, 260 (317); 133, 277 (327 f.).

Der Umstand, dass die letztendliche Identifizierung durch Menschen vorgenommen wird und (jedenfalls bei der Verwendung des BKA-GES) nur geschulte Experten diese Kontrolle durchführen, erscheint grundsätzlich geeignet, das Eingriffsgewicht zu verringern (oder die Fehleranfälligkeit weniger stark ins Gewicht fallen zu lassen). Allerdings ist die Überprüfung durch Menschen gesetzlich nicht festgelegt,[449] sodass es letztlich eine Entscheidung der Strafverfolgungsbehörden bleibt, ob und wie diese vorgenommen wird. Auch ist nicht offiziell bekannt, wie die Polizeibehörden, die zusätzlich noch eigene Gesichtserkennungssysteme einsetzen, die menschliche Kontrolle handhaben.

Jedenfalls ist aber mindernd zu berücksichtigen, dass die zum Abgleich herangezogene Datenbank zwar umfangreich (6,7 Millionen Bilder), doch zumindest begrenzt ist. Anders als bei der automatisierten Kfz-Kennzeichenkontrolle oder bei einer Echtzeit-Fahndung per Gesichtserkennung im öffentlichen Raum werden daher zumindest nicht alle vorbeilaufenden oder -fahrenden Personen wahllos erfasst. Auch diese Begrenzung der Datenbank ist allerdings in keiner gesetzlichen Grundlage festgelegt.[450]

Dagegen reduziert der Umstand, dass der Abgleich erst im Nachhinein (statt in Echtzeit) erfolgt, *nicht* per se das Eingriffsgewicht.[451] In diese

449 Daher erscheint dieser Umstand nur begrenzt berücksichtigungsfähig, vgl. in diese Richtung BVerfGE 115, 320 (354).

450 Insbesondere die für Gesichtserkennung herangezogene Vorschrift des § 98c StPO begrenzt die Datenbanken nicht näher; sie erlaubt einen maschinellen Abgleich „personenbezogene[r] Daten aus einem Strafverfahren mit anderen zur Strafverfolgung oder Strafvollstreckung oder zur Gefahrenabwehr gespeicherten Daten".

451 Mit Blick auf die Vorratsdatenspeicherung vertrat der EuGH die Auffassung, dass der „Eingriff, der mit einer Erhebung von Daten, die es ermöglichen, den Standort eines Endgeräts zu ermitteln, in Echtzeit verbunden ist, […] besonders schwerwiegend [ist], denn diese Daten versetzen die zuständigen nationalen Behörden in die Lage, die Ortsveränderungen der Nutzer von Mobiltelefonen präzise und permanent nachzuverfolgen. Da diese Daten somit als besonders sensibel einzustufen sind, ist der Echtzeit-Zugang der zuständigen Behörden zu solchen Daten von einem zeitversetzten Zugang zu ihnen zu unterscheiden; Ersterer ist einschneidender, weil er eine nahezu perfekte Überwachung dieser Nutzer erlaubt […]", EuGH, Urt. v. 6.10.2020, La Quadrature du Net ua/Premier ministre ua sowie Ordre des barreaux francophones et germanophone ua/Conseil des Ministres, C-511/18, C-512/18, C-520/18, Rn. 187. Auch hier ist es jedoch nicht die Echtzeit-Auswertung als solche, sondern die – notwendig nachträgliche – Zusammenführung der Informationen, die es erlaubt, ein präzises Bewegungsprofil zu erstellen. Die Echtzeit-Auswertung zeigt hingegen nur, wo die Person sich derzeit befindet. Und erneut: Um eine Echtzeit-Datenerhebung würde es sich auch dann handeln, wenn die Standortdaten in Echtzeit erfasst, aber wenige Minuten später wieder gelöscht würden. Auch das

Richtung geht aber die KI-Verordnung auf EU-Ebene, die zwischen nachträglicher und Echtzeit-Fernidentifizierung (im öffentlichen Raum zu Zwecken der Strafverfolgung) unterscheidet und die nachträgliche Fernidentifizierung pauschal als weniger eingriffsintensiv ansieht.[452] Begründet wird das höhere Eingriffsgewicht der Echtzeit-Fernidentifizierung dort mit der „Unmittelbarkeit der Auswirkungen und [den] [...] begrenzten Möglichkeiten weiterer Kontrollen oder Korrekturen" und damit zusammenhängend „erhöhte[n] Risiken für die Rechte und Freiheiten der betreffenden Personen, die im Zusammenhang mit Strafverfolgungsmaßnahmen stehen oder davon betroffen sind" (ErwG 32). Zudem greife Echtzeit-Fernidentifizierung natürlicher Personen in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken besonders in die Rechte und Freiheiten der betroffenen Personen ein, da sie „die Privatsphäre eines großen Teils der Bevölkerung beeinträchtigt, ein Gefühl der ständigen Überwachung weckt und indirekt von der Ausübung der Versammlungsfreiheit und anderer Grundrechte abhalten kann" (ErwG 32). Auch in der deutschen verfassungsrechtlichen Literatur wird mit Blick auf Gesichtserkennung der Faktor, dass die Auswertung im Nachhinein erfolgt, neben anderen Umständen als mildernd erwähnt.[453] Die nachträgliche Anwendung von Gesichtserkennung zur Aufklärung von Straftaten ist zwar weniger eingriffsintensiv als die Echtzeit-Videoüberwachung per Gesichtserkennung im öffentlichen Raum. Die *Nachträglichkeit* der Auswertung ist dabei aber kein entscheidender Faktor. Der Grund, warum eine Videoüberwachung mit Gesichtserkennung im öffentlichen Raum so eingriffsintensiv ist, liegt an der Streubreite (am öffentlichen Raum), nicht an der Echtzeit der Auswertung. Würden diese Videos von Flughäfen, Bahnhöfen und anderen öffentlichen Plätzen erst Stunden,

---

ist nicht zwingend eingriffsintensiver als Daten erst zeitversetzt (z. B. Stunden oder Tage später), aber dafür gesammelt und in großem Umfang zu erheben, um sie dann zusammenführen zu können. Eine Verkürzung auf „Datenerhebung in Echtzeit ist immer eingriffsintensiver" sollte daher auch aus dieser Entscheidung des EuGH nicht abgeleitet werden.

452 Dazu kritisch bereits *Hahn*, ZfDR 2023, 142, 155 ff.; ähnlich kritisch auch *Rostalski/Weiss*, in: Hilgendorf/Roth-Isigkeit, Die neue Verordnung der EU zur Künstlichen Intelligenz, 2023, 35 (44); *Linardatos*, GPR 2022, 58, 62; *Schindler/Schomberg*, in: Friedewald/Roßnagel/Heesen/Krämer/Lamla, Künstliche Intelligenz, Demokratie und Privatheit, 2022, 103, 121; *Rostalski/Weiss,* ZfDR 2021, 329, 344. Anders *Tschorr*, MMR 2024, 304, 307, die hierfür entscheidend auf die „Unmittelbarkeit der Identifikation [...], die keinen Spielraum für menschliche Interaktion lässt", abstellt.

453 Vgl. etwa *Martini/Thiessen/Ganter*, Digitale Versammlungsbeobachtung, 2023, 95, Fn. 451, 111 f.; *Petri*, GSZ 2018, 144, 148; *Kulick*, NVwZ 2020, 1622, 1625.

Tage, Wochen oder Monate später per Gesichtserkennung ausgewertet, dann läge hierin kein geringerer Eingriff. Womöglich wäre der Eingriff sogar ein tieferer, da bedeutend mehr Informationen über einen Menschen bekannt und verknüpft werden könnten, etwa auch, um ein Bewegungs- oder Persönlichkeitsprofil zu erstellen.[454] Um eine Echtzeitauswertung handelt es sich dagegen auch, wenn die Personen zwar live per Gesichtserkennung mit einer Fahndungsliste abgeglichen werden, die Videoaufnahmen und die biometrischen Daten aber sofort danach automatisch gelöscht werden, sofern kein Treffer vorliegt. Das ist sicher nicht eingriffsintensiver als eine umfangreiche nachträgliche Auswertung der Aufnahmen im öffentlichen Raum.

c) Fazit

Der Einsatz von Gesichtserkennung zur Identifizierung unbekannter Verdächtiger geht mit Eingriffen in das Recht auf informationelle Selbstbestimmung einher. Eigenständige Eingriffe begründen die Erstellung der Embeddings, der Abgleich mit den Embeddings der in der durchsuchten Datenbank gespeicherten Personen sowie die Treffer (Auftauchen auf der Kandidatenliste).

Dabei kommt jedenfalls dem Abgleich und den Treffern ein erhebliches Eingriffsgewicht zu. Grund dafür sind vor allem die Heimlichkeit, Streubreite und Anlasslosigkeit, Anknüpfung an höchstpersönliche körperliche Merkmale und die drohenden Folgeeingriffe. Nachrangig könnten auch Einschüchterungseffekte und die grundsätzliche leichte Verknüpfbarkeit von Informationen durch Gesichtserkennung herangezogen werden. Sinnvoll erscheint es zudem, die spezifische Fehleranfälligkeit von Gesichtserkennung als eigenes Kriterium verstärkt eingriffserhöhend zu berücksichti-

454 *Hahn*, ZfDR 2023, 142, 155 f. Zudem werden bei der Echtzeit-Auswertung nur Aufnahmen durchleuchtet, die aktuell zu staatlichen Zwecken angefertigt werden, da nur dann die Erfassung biometrischer Daten (also etwa die Videoaufnahme), der Abgleich und die Identifizierung „ohne erhebliche Verzögerung" erfolgen. Bei der nachträglichen Auswertung kann hingegen auch Bild- und Videomaterial, das ursprünglich zu anderen Zwecken erstellt wurde, „umgewidmet" und daher viel mehr Datenmaterial herangezogen werden; hierzu bereits *Hahn*, ZfDR 2023, 142, 156.

gen.[455] Das Eingriffsgewicht reduzierend wirkt sich insbesondere aus, dass zwar Daten vieler überwiegend nicht beteiligter Personen einbezogen werden, der Datenabgleich aber in Sekundenschnelle durchgeführt wird und die erfassten Daten im Nichttrefferfall keine weitere polizeiliche Tätigkeit veranlassen. Insgesamt ist daher jedenfalls mit Blick auf den Abgleich per Gesichtserkennung und die Treffer von einem erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung auszugehen.

Auch der Eingriff durch Treffer ist erheblich. Er zeichnet sich zwar durch eine geringere Streubreite als der Abgleich aus, jedoch besteht bei einem Treffer die bereits sehr konkrete Gefahr, fehlerhaft identifiziert und Folgemaßnahmen unterworfen zu werden. Der Eingriff durch die Erstellung der Embeddings hat dagegen eine etwas geringere Eingriffsintensität, denn die Gefahr von Folgemaßnahmen ist hier noch nicht konkretisiert.

455 Der Umstand, dass automatisierte Gesichtserkennung auf Methoden des maschinellen Lernens und damit der Künstlichen Intelligenz beruht, dürfte sich hingegen nicht zusätzlich eingriffserhöhend auswirken. Richtigerweise hat das Bundesverfassungsgericht in der Entscheidung zur automatisierten Datenanalyse den Einsatz von Künstlicher Intelligenz nicht per se als Eingriffsgewicht erhöhenden Faktor angesehen, BVerfGE 165, 363 (408) („Besonderes Eingriffsgewicht *kann* je nach Einsatzart die Verwendung lernfähiger Systeme, also Künstlicher Intelligenz (KI), haben." (Hervorhebung J. H.)). Zwar sind Gesichtserkennungssysteme insofern „selbstlernend", als dass sie die für die Gesichtserkennung relevanten Gesichtsmerkmale selbst herausfinden und festlegen. Nachdem sie „austrainiert" sind, werden diese Systeme aber nicht mehr weitertrainiert und lernen nicht mehr weiter. Bei Gesichtserkennungssystemen besteht außerdem – anders als bei anderen KI-Systemen – nicht die Gefahr, dass sie neue, nicht nachvollziehbare Zusammenhänge erschaffen. Sie können ausschließlich eine Aussage über die Ähnlichkeit von Face Embeddings (also von Gesichtern) treffen.

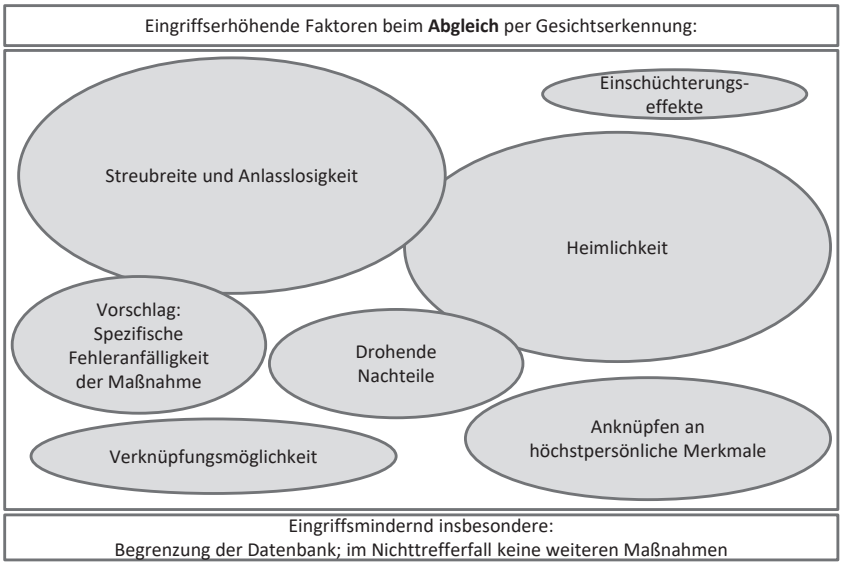

Abbildung 4: Eingriffsgewicht bestimmende Faktoren beim Abgleich mit Gesichtserkennung

3. Rechtfertigung

Das Recht auf informationelle Selbstbestimmung ist Schranken unterworfen, denn der Einzelne hat als eine „sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeit" über seine Daten „nicht ein Recht im Sinne einer absoluten, uneinschränkbaren Herrschaft".[456] Es stellt sich daher die Frage, welche Anforderungen an eine Rechtfertigung der oben festgestellten erheblichen Eingriffe zu stellen sind. Mit anderen Worten: Wie muss eine gesetzliche Grundlage ausgestaltet sein, auf die der Einsatz automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger gestützt werden darf? Die Ermächtigungen für die verschiedenen Eingriffe (etwa Erhebung, Abgleich und Verwendung von Daten) müssen nicht in verschiedenen Rechtsgrundlagen, sondern können in einer Vorschrift zusammengefasst geregelt sein.

456 BVerfGE 65, 1 (43 f.).

Bei besonders eingriffsintensiven Maßnahmen schränkt das Bundesverfassungsgericht den Spielraum des Gesetzgebers teilweise stark ein und gibt ihm nahezu „eine gesetzliche Regelung bis in die Einzelheiten nach Art einer Handlungsanleitung vor".[457] Ungeachtet der Frage, ob dies nicht einem oft behaupteten, freilich unscharfen Gebot verfassungsrichterlicher Zurückhaltung zuwiderläuft,[458] erreicht jedenfalls der Einsatz von Gesichtserkennung zur Identifizierung unbekannter Verdächtiger eine solche Eingriffsintensität nicht. Insbesondere wird, anders als etwa bei der Telekommunikationsüberwachung (§ 100a StPO), der Kernbereich privater Lebensgestaltung kaum je betroffen sein. Dem Gesetzgeber wird daher grundsätzlich ein beträchtlicher Regelungsspielraum zuzubilligen sein; wie dieser sinnvollerweise genutzt werden könnte, wird in Kapitel IV. besprochen. Die wichtigen verfassungsrechtlich zwingenden Leitlinien hingegen sollen im Folgenden dargestellt werden.[459]

Die Ermächtigungsgrundlage ist insbesondere am Verhältnismäßigkeitsgrundsatz zu messen und muss insbesondere im Bereich der Datenverarbeitung den Geboten der Bestimmtheit und Normenklarheit genügen. Darüber hinaus sind gerade bei heimlichen Maßnahmen Vorgaben zu Verfahren, Organisation und Kontrolle zu machen.

a) Verhältnismäßigkeit

Die Ermächtigungen für Grundrechtseingriffe müssen einen legitimen Zweck verfolgen, zur Erreichung des Zwecks geeignet, erforderlich und verhältnismäßig im engeren Sinne (angemessen) sein.[460]

457 Sondervotum Schluckebier, BVerfGE 125, 260 (369); kritisch etwa auch Sondervotum Eichberger, BVerfGE 125, 260 (383).

458 So Sondervotum Schluckebier, BVerfGE 125, 260 (373).

459 Ob eine bestehende Vorschrift diesen Anforderungen genügt und daher für die Identifizierung unbekannter Verdächtiger per Gesichtserkennung herangezogen werden kann, wird nachfolgend näher untersucht (Kapitel II. C. Bestehen einer Rechtsgrundlage).

460 BVerfGE 67, 157 (173); 120, 378 (427); 141, 220 (265); stRspr.

aa) Verfolgbare Straftaten

Der Verhältnismäßigkeitsgrundsatz kann auch den Spielraum des Gesetzgebers dahingehend einschränken, welche Straftaten mit welcher Maßnahme verfolgt werden dürfen.[461] Bei Maßnahmen hoher und besonders hoher Eingriffsintensität fordert das Bundesverfassungsgericht eine Beschränkung auf einen gesetzlichen Katalog schwerer Straftaten.[462] Um eine Maßnahme so hoher Intensität handelt es sich aber beim Einsatz von Gesichtserkennung zur Identifizierung von Tätern nicht.

bb) Geeignetheit

Auch aus dem Erfordernis der Geeignetheit ergibt sich nichts anderes. Automatisierte Gesichtserkennung kann zur Aufklärung jedes Delikts grundsätzlich hilfreich sein, sofern ein unbekannter Täter zu identifizieren ist. Der Geeignetheit von Gesichtserkennung zur Ermittlung der Identität unbekannter Verdächtiger steht im Übrigen nicht entgegen, dass die Person hierdurch nicht unmittelbar identifiziert, sondern nur eine Vorauswahl getroffen wird. Denn die Wahrscheinlichkeit, die Person zu identifizieren, wird jedenfalls erhöht.[463] Aus diesem Grund steht auch die Möglichkeit von falsch-positiven Treffern oder falschen Nichttreffern der Geeignetheit nicht entgegen.

cc) Erforderlichkeit

Der Erforderlichkeit des Einsatzes von Gesichtserkennung steht insbesondere nicht entgegen, dass auch auf sog. Super Recognizer[464] zurückgegriffen werden könnte. Dies ist nicht gleich effektiv, da diese Menschen zwar besondere Fähigkeit bei der Wiedererkennung von Personen haben, aber anders als die Maschine nicht in Sekunden Millionen von Gesichtsbildern durchsuchen können.

461 Vgl. nur *Bäcker*, in: Herdegen/Masing/Poscher/Gärditz, Handbuch des Verfassungsrechts, 2021, § 28 Sicherheitsverfassungsrecht, Rn. 105.
462 Um die Schwere einer Straftat abstrakt zu bestimmen, greift das Gericht auf den gesetzlichen Strafrahmen zurück, siehe etwa BVerfGE 129, 208.
463 Vgl. zu einer ähnlichen Begründung BVerfGE 150, 244 (280).
464 Zu diesen bereits Kapitel I. G. I. 1.

b) Bestimmtheit und Normenklarheit

Die Rechtsgrundlage muss zudem insbesondere im Bereich der Datenverarbeitung dem Gebot der Bestimmtheit und Normenklarheit genügen.[465] Mit Blick auf die informationelle Selbstbestimmung konkretisiert das Gericht zudem, dass „der Anlass, der Zweck und die Grenzen" des Eingriffs „bereichsspezifisch, präzise und normenklar" festgelegt werden müssen.[466] Das Gebot der Bestimmtheit und Normenklarheit dient der Vorhersehbarkeit von Eingriffen für die Bürger, einer wirksamen Begrenzung der Befugnisse sowie der Ermöglichung einer effektiven Kontrolle durch die Gerichte.[467] Zudem soll durch dieses Prinzip sichergestellt werden, dass der demokratisch legitimierte Gesetzgeber die wesentlichen Entscheidungen über Grundrechtseingriffe und deren Reichweite selbst trifft (Wesentlichkeitsprinzip). Jedenfalls mit Blick auf heimliche Maßnahmen ist nach der neuen Rechtsprechung zwischen der Bestimmtheit einerseits und der Normenklarheit andererseits zu unterscheiden.[468]

Bei der Bestimmtheit geht es vor allem darum, dass die Exekutive im Gesetz steuernde und begrenzende Handlungsmaßstäbe vorfindet und dass eine wirksame Rechtskontrolle durch die Gerichte möglich ist.[469] Der Gesetzgeber hat die Regelungen so bestimmt zu fassen, wie dies nach der Eigenart des zu ordnenden Lebenssachverhalts mit Rücksicht auf den Normzweck möglich ist.[470] Ausreichend ist es, wenn durch Auslegung der Vorschriften mithilfe der anerkannten Auslegungsregeln feststellbar ist, ob die tatsächlichen Voraussetzungen für die in der Rechtsnorm ausgesprochene Rechtsfolge vorliegen.[471] Dem Bestimmtheitserfordernis ist daher genügt,

465 Vgl. BVerfGE 113, 348 (375 ff.); 120, 378 (407 f.); 141, 220 (265); stRspr.

466 BVerfGE 113, 348 (375); 128, 1 (47); 130, 151 (202); zur Übertragung dieses Erfordernisses auf Art. 10 GG Dürig/Herzog/Scholz/*Durner*, 102. EL August 2023, GG Art. 10 Rn. 176.

467 BVerfGE 156, 11 (44 f.); 113, 348 (375 ff.); 120, 378 (407 f.)

468 So nun der Erste Senat in BVerfGE 156, 11 (44 f.), der in dieser Hinsicht zuvor aber noch nicht differenziert hatte, siehe etwa BVerfGE 113, 348 (375 ff.); 118, 168 (168 ff.). Vgl. hierzu auch BVerfG (Zweiter Senat), Urt. v. 29.11.2023, 2 BvF 1/21, BeckRS 2023, 33683 Rn. 81.

469 Siehe z. B. BVerfGE 156, 11 (45).

470 Vgl. BVerfGE 49, 168 (181); 78, 205 (212); 102, 254 (337); 145, 20 (69 f.); stRspr.

471 Allerdings dürfen verbleibende Unsicherheiten nicht dazu führen, dass die Vorhersehbarkeit und Justiziabilität des Handelns der durch die Norm ermächtigten staatlichen Stellen gefährdet sind, BVerfGE 156, 11 (45) mwN.

wenn die Auslegungsprobleme mit herkömmlichen juristischen Methoden bewältigt werden können.[472]

Dagegen steht bei der Normenklarheit die inhaltliche Verständlichkeit der Regelung im Vordergrund, dies vor allem damit Bürger sich auf mögliche belastende Maßnahmen einstellen können.[473] In der Entscheidung Antiterrordateigesetz II versteht der Erste Senat die Normenklarheit, soweit ersichtlich, erstmals als eigenständiges und unter Umständen strengeres Gebot als die Bestimmtheit.[474] Inhaltlich sind die Anforderungen an die Normenklarheit jedoch nicht neu; sie wurden, auch in derselben Formulierung, bereits zuvor schon im Rahmen eines einheitlich betrachteten „Grundsatz[es] der Normenklarheit und Bestimmtheit" gestellt.[475] Besonders strenge Anforderungen gelten danach bei der heimlichen Datenerhebung und -verarbeitung, die tief in die Privatsphäre einwirken können.[476] Dies wird damit begründet, dass die Handhabung heimlicher Maßnahmen von den Betroffenen weitgehend nicht wahrgenommen und angegriffen werden könne, sodass ihr Gehalt nur sehr eingeschränkt im Wechselspiel von Anwendungspraxis und gerichtlicher Kontrolle konkretisiert werden könne.[477] Die Anforderungen an die Normenklarheit unterscheiden sich vor allem nach dem Eingriffsgewicht und sind mit den jeweiligen materiellen Anforderungen der Verhältnismäßigkeit eng verbunden. Bei heimlichen Maßnahmen müsse der Inhalt der einzelnen Norm verständlich und ohne größere Schwierigkeiten durch Auslegung zu konkretisieren sein, da hier die Grundrechte ohne Wissen der Bürger und oft ohne die Erreichbarkeit gerichtlicher Kontrolle eingeschränkt würden.[478] Daher könne eine Regelung durch Auslegung bestimmbar oder der verfassungskonformen Auslegung zugänglich und damit im Verfassungssinne „bestimmt" sein (also dem Bestimmtheitsgebot genügen), jedoch gehe damit nicht zwingend auch ihre

472 Siehe nur mwN BVerfGE 134, 141 (184); 156, 11 (45).
473 Vgl. BVerfGE 145, 20 (69 f.); 156, 11 (45).
474 BVerfGE 156, 11 (45 f.).
475 So etwa in BVerfGE 141, 220 (265).
476 BVerfGE 156, 11 (45); so auch in BVerfGE 163, 43 (83).
477 BVerfGE 156, 11 (45). Mit dieser Formulierung aber etwa auch BVerfGE 141, 220 (265), wo noch nicht zwischen Normenklarheit und Bestimmtheit differenziert wird. Treffend dazu *Bäcker*, in: Herdegen/Masing/Poscher/Gärditz, Handbuch des Verfassungsrechts, 2021, § 28 Sicherheitsverfassungsrecht, Rn. 87: Die Rechtsgrundlage müsse selbst „bereits eine erhebliche Konkretisierungsleistung erbringen".
478 BVerfGE 156, 11 (46).

Normenklarheit für die Adressaten einher[479].[480] Bei einer Ermächtigungsgrundlage zum Einsatz von Gesichtserkennung als heimlicher Maßnahme sind diese erhöhten Anforderungen an die Normenklarheit daher ebenfalls zu beachten. Dabei sind aber etwas geringere Anforderungen zu stellen bei noch eingriffsintensiveren Maßnahmen wie etwa der akustischen Wohnraumüberwachung. Mit Blick auf technologische Entwicklungen verlangt das Bundesverfassungsgericht keine gesetzlichen Formulierungen, die jede Einbeziehung kriminaltechnischer Neuerungen ausschließen.[481] Wegen des schnellen und für den Grundrechtsschutz riskanten informationstechnischen Wandels müsse der Gesetzgeber aber „die technischen Entwicklungen aufmerksam beobachten und bei Fehlentwicklungen hinsichtlich der konkreten Ausfüllung offener Gesetzesbegriffe durch die Strafverfolgungsbehörden und die Strafgerichte notfalls durch ergänzende Rechtssetzung korrigierend eingreifen".[482] Dies betreffe auch die Frage, ob die bestehenden verfahrensrechtlichen Vorkehrungen – wie etwa Benachrichtigungspflich-

479 So habe die Rechtsprechung etwa lange und intransparente Verweisungsketten als Verstoß gegen die Normenklarheit angesehen, so BVerfGE 156, 11 (46) unter Verweis auf BVerfGE 110, 33 (57, 62 f.); 154, 152 (266 Rn. 215).

480 BVerfGE 156, 11 (46). Siehe aber hingegen die Auffassung des Zweiten Senats in BVerfG (Zweiter Senat), Urt. v. 29.11.2023, 2 BvF 1/21, BeckRS 2023, 33683 (LS 1): „Bei dem Gebot hinreichender Bestimmtheit und Klarheit der Gesetze handelt es sich um ein einheitliches Postulat, das verschiedene Aspekte in sich vereint. Demgemäß ist der Maßstab hierfür einheitlich zu bestimmen; eine Trennung zwischen Bestimmtheits- und Klarheitsgebot dahingehend, dass eine Norm zwar noch hinreichend bestimmt sein kann, dennoch aber gegen das Gebot der Normenklarheit verstößt, kommt *grundsätzlich* nicht in Betracht" (Hervorhebung J. H.). Dieser Sichtweise, so der Zweite Senat, stehe die Auffassung des Ersten Senats in BVerfGE 156, 11 nicht entgegen. Denn diese Ausführungen seien auf die von ihm, dem Zweiten Senat, zu entscheidende Konstellation nicht übertragbar. In der Entscheidung des Ersten Senats sei es um heimliche Eingriffe gegangen, bei denen eine gerichtliche Kontrolle oft nur eingeschränkt möglich sei. Bei der Entscheidung des Zweiten Senats gehe es hingegen nicht um heimliche Grundrechtseingriffe, sondern um Vorschriften, die die Umrechnung von bei der Wahl zum Deutschen Bundestag abgegebenen Stimmen in Parlamentssitze regeln; auch sei nicht die Wahlhandlung als solche betroffen. Das Erfordernis einer eigenständigen und strengeren Kontrolle der Normenklarheit primär von der Frage abhängig zu machen, ob der Eingriff heimlich erfolgt und (oder?) ob gerichtliche Kontrolle regelmäßig möglich ist, erscheint *prima facie* nicht zwingend. Auch in anderen Konstellationen kann es ein besonderes Bedürfnis der Bürger dafür geben, dass eine Norm für sie (vergleichsweise) verständlich ist.

481 BVerfGE 112, 304 (316).

482 BVerfGE 112, 304 (316 f.); vgl. auch BVerfGE 90, 145 (191); BVerfG, NJOZ 2021, 1391, 1396.

ten oder Rechtsschutzmöglichkeiten – angesichts zukünftiger Entwicklungen geeignet sind, den Grundrechtsschutz effektiv zu sichern.[483]

Zunächst muss eine Rechtsgrundlage, auf die eine automatisierte Gesichtserkennung gestützt wird, daher deutlich machen, dass ein automatisierter Abgleich von Daten durchgeführt wird. Zudem muss sie erkennen lassen, welche Arten von Daten abgeglichen werden dürfen. Dies betrifft zum einen die Frage, um welche Art von Daten es sich handelt. Wie oben erläutert, handelt es sich bei den Gesichtsmerkmalen (die zur Gesichtserkennung in Embeddings extrahiert werden) nicht nur um personenbezogene, sondern um biometrische Daten, die außerdem noch weitgehend unveränderlich und individuell sind und einem Menschen immer und überall hin „folgen". Aus Gründen der Bestimmtheit und Normenklarheit muss eine Rechtsgrundlage daher zumindest deutlich machen, dass biometrische Merkmale verwendet werden; angesichts der Einzigartigkeit und weitgehenden Unveränderlichkeit des menschlichen Gesichts könnte es sogar erforderlich sein, dies näher zu spezifizieren und von Gesichtsmerkmalen zu sprechen. Zum anderen muss aus der Ermächtigungsgrundlage ersichtlich sein, welche Datensätze abgeglichen werden dürfen, also welche polizeilichen Datenbanken herangezogen werden dürfen. Nur dann ist für die Bürger ersichtlich, dass sie von der Maßnahme betroffen sein könnten. Mit Blick auf den Zweck muss die Ermächtigungsgrundlage insbesondere festlegen, dass der Abgleich zur Identifizierung unbekannter Verdächtiger dient; diese nähere Zweckbeschreibung würde zugleich deutlich machen, dass der Einsatz von Gesichtserkennung etwa zur Echtzeit-Fahndung nicht erfasst ist. Dies dient zugleich der Verwirklichung des Wesentlichkeitsprinzips[484], wonach der parlamentarische Gesetzgeber alle wichtigen (wesentlichen) Entscheidungen mit Blick auf Art und Ausmaß der Grundrechtsbeeinträchtigung selbst zu treffen hat.

c) Verfahren und Organisation

Die Heimlichkeit einer Maßnahme und die damit einhergehende fehlende Transparenz müssen durch besondere Vorgaben zu Verfahren und Organi-

483 BVerfG, NJOZ 2021, 1391 (1396).
484 Vgl. nur BVerfGE 49, 89 LS. 2.

sation kompensiert werden.[485] Für die Gesichtserkennung kommen insbesondere Benachrichtigungspflichten, ein Richtervorbehalt, eine aufsichtliche Kontrolle und Berichts- und Evaluationspflichten in Betracht.

aa) Richtervorbehalt

Das Bundesverfassungsgericht hält allerdings in seiner Rechtsprechung eine vorherige Bewilligung durch eine unabhängige Stelle, insbesondere ein Gericht, bei heimlichen Ermittlungsmaßnahmen verfassungsrechtlich nur für erforderlich, wenn der Eingriff „schwerwiegend"[486] bzw. von „besonders hohe[r] Eingriffsintensität" ist, insbesondere wenn zu erwarten ist, dass höchstprivate Informationen erfasst werden.[487] Ob der Einsatz automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger ein so schwerwiegender Grundrechtseingriff ist, dass es eines Richtervorbehalts bedürfte, ist fraglich;[488] höchstprivate Informationen werden in den seltensten Fällen erfasst. Aus kriminalpolitischen Gründen erscheint eine vorherige Bewilligung der Gesichtserkennung durch ein Gericht jedoch sinnvoll (hierzu näher Kapitel IV.).[489]

bb) Benachrichtigungspflicht

Grundsätzlich hat der Gesetzgeber sicherzustellen, dass die von einer heimlichen Maßnahme Betroffenen jedenfalls im Nachhinein von dieser erfahren können (etwa durch Auskunftsrechte) und so in die Lage versetzt werden, gegebenenfalls Rechtsschutz zu suchen.[490] Zudem ist eine (akti-

485 Vgl. auch *Bäcker*, in: Herdegen/Masing/Poscher/Gärditz, Handbuch des Verfassungsrechts, 2021, § 28 Sicherheitsverfassungsrecht, Rn. 110; *Eifert*, in: Herdegen/Masing/Poscher/Gärditz, Handbuch des Verfassungsrechts, 2021, § 18 Persönliche Freiheit, Rn. 129; *Heckmann/Paschke*, in: Stern/Sodan/Möstl, Das Staatsrecht der Bundesrepublik Deutschland im europäischen Staatenverbund, 2. Aufl. 2022, § 103 Datenschutz, Rn. 47.

486 Vgl. nur BVerfGE 125, 260 (337); hierzu auch BeckOK InfoMedienR/*Gersdorf*, 42. Ed., Stand: 1.5.2021, GG Art. 2 Rn. 88.

487 Vgl. nur BVerfGE 141, 220 (294).

488 Ablehnend *Schindler*, Biometrische Videoüberwachung, 2021, 614.

489 Kapitel IV. B. II. 2.

490 *Bäcker*, in: Herdegen/Masing/Poscher/Gärditz, Handbuch des Verfassungsrechts, 2021, § 28 Sicherheitsverfassungsrecht, Rn. 110.

ve) Benachrichtigung durch die Strafverfolgungsbehörden bei heimlichen Maßnahmen typischerweise verfassungsrechtlich geboten, wenn es sich um einen heimlichen Grundrechtseingriff von erheblichem Gewicht handelt und andere Kenntnismöglichkeiten den Interessen des Betroffenen nicht hinreichend Rechnung tragen.[491] Nach überzeugender neuerer bundesverfassungsgerichtlicher Rechtsprechung dürfte bei heimlichen Maßnahmen eine Benachrichtigungspflicht sogar der Regelfall sein, nur bei Eingriffen geringer Intensität bedarf es einer solchen nicht.[492] Mit Blick auf automatisierte Kfz-Kennzeichenkontrollen hat es das Bundesverfassungsgericht angesichts des im Vergleich mit anderen heimlichen Maßnahmen geringeren Eingriffsgewichts eine Benachrichtigungspflicht auch im Trefferfall nicht für erforderlich gehalten. Unter Verhältnismäßigkeitsgesichtspunkten genüge es, „wenn die Betroffenen von den Kontrollen nur im Rahmen von ihnen gegenüber ergriffenen Folgemaßnahmen erfahren und deren Rechtmäßigkeit dann fachgerichtlich überprüfen lassen können".[493] In welcher Form die Betroffenen bei den Folgemaßnahmen dann von der Kennzeichenkontrolle „erfahren" sollen, wird nicht näher festgelegt.

Mit Blick auf die automatisierte Gesichtserkennung muss differenziert werden zwischen den Personen, die in der durchsuchbaren Datenbank gespeichert sind und abgeglichen werden, den „Treffern", die auf der Kandidatenliste erscheinen und den Personen, gegen die weitere Maßnahmen ergriffen werden. Hinsichtlich der abgeglichenen Personen ist eine Benachrichtigung bereits nicht praktikabel,[494] da hierfür mehrmals täglich Millionen von Menschen kontaktiert werden müssten.[495] Auch erscheint es verfassungsrechtlich nicht zwingend, die auf der Liste auftauchenden Personen zu benachrichtigen, denn dazu müssten zunächst deren Namen und Adressen anhand der INPOL-Eintragung festgestellt werden; das wür-

491 Vgl. BVerfGE 65, 1 (70); 100, 313 (361); 109, 279 (363 f.); 118, 168 (208); 120, 351 (363). Hierzu zu Recht kritisch *Schwabenbauer*, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, Kapitel G. Informationsverarbeitung im Polizei- und Strafverfahrensrecht, Rn. 321.

492 BVerfGE 130, 151 (210); 155, 119 (226). So auch *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, 2023, 168.

493 BVerfGE 150, 244 (302).

494 Zu diesem Gedanken im Zusammenhang mit der automatischen Kennzeichenerfassung BT-Drs. 19/27654, 72.

495 Zur Vereinbarkeit einer solchen Ausnahme von der Benachrichtigungspflicht für nur unerheblich betroffene Personen mit Art. 13 JI-RL *Schindler*, Biometrische Videoüberwachung, 2021, 717.

de den Grundrechtseingriff noch vertiefen.[496] Allerdings erscheint es verfassungsrechtlich geboten, die Person, gegen die weiter ermittelt werden soll, zu benachrichtigen. Bei der Rasterfahndung nach § 98a StPO oder der Schleppnetzfahndung nach § 163d StPO sind etwa Benachrichtigungspflichten geregelt für „die betroffenen Personen, gegen die nach Auswertung der Daten weitere Ermittlungen geführt wurden";[497] die Benachrichtigung kann in Ausnahmefällen unterbleiben[498] oder zurückgestellt werden[499]. Eine solche grundsätzliche Benachrichtigungspflicht sollte auch für den Einsatz von Gesichtserkennung geregelt werden. Dies legt nicht nur das Eingriffsgewicht nahe, sondern auch die spezifische Fehleranfälligkeit von Gesichtserkennung. Der Betroffene muss daher ausdrücklich darüber informiert sein, dass Ermittlungen sich gegen ihn deshalb richten, weil er dem unbekannten Verdächtigen ähnlich sieht und er daher nach einer Gesichtserkennungsrecherche identifiziert wurde. Ein bloßes Auskunftsrecht, für dessen Wahrnehmung der Betroffene womöglich gar keinen Anlass sieht, ist bei einer so eingriffsintensiven und fehleranfälligen Maßnahme nicht ausreichend. Verfassungsrechtlich erscheint eine (aktive) Benachrichtigungspflicht mit Blick auf den nun Verdächtigten daher geboten.[500]

cc) Kontrolle

Bereits im Volkszählungsurteil hielt das Bundesverfassungsgericht fest, dass „[w]egen der für den Bürger bestehenden Undurchsichtigkeit der Speicherung und Verwendung von Daten unter den Bedingungen der automatischen Datenverarbeitung und auch im Interesse eines vorgezogenen Rechtsschutzes durch rechtzeitige Vorkehrungen […] die Beteiligung unabhängiger Datenschutzbeauftragter von erheblicher Bedeutung für einen effektiven Schutz des Rechts auf informationelle Selbstbestim-

496 In diese Richtung auch BVerfGE 109, 279 (365).

497 Siehe § 101 Abs. 4 S. 1 Nr. 1 und 10 StPO. Hierzu auch MüKoStPO/*Rückert*, 2. Aufl. 2023, StPO § 101 Rn. 24 und 49. Dies umfasst alle Personen, gegen die sich aufgrund der Datenverarbeitung ein Tatverdacht ergeben hatte, unabhängig davon, ob sich dieser bestätigt hat oder nicht, vgl. *Kahmen*, Die Vorschriften zur Benachrichtigungspflicht gemäß § 101 IV-VI StPO und ihre praktische Umsetzung, 2017, 105 f.

498 § 101 Abs. 4 S. 3 bis 5 StPO und § 101 Abs. 6 S. 3 StPO zum endgültigen Absehen von der Benachrichtigung nach Zurückstellungen.

499 Vgl. zum Zeitpunkt der Benachrichtigung § 101 Abs. 5 und 6 StPO.

500 Zur kriminalpolitischen Ausgestaltung siehe Kapitel IV. B. II. 1.

mung" ist.[501] Dadurch soll eine nachträgliche Kontrolle[502] der Verwendung der Daten und ein Schutz vor Missbrauch sichergestellt werden.[503] Eine Kontrolle durch den Bundes- oder Landesdatenschutzbeauftragten, teilweise auch durch behördliche Datenschutzbeauftragte hat das Bundesverfassungsgericht in der Vergangenheit als ausreichend angesehen.[504] Allerdings ist zweifelhaft, ob dies für den Einsatz von Gesichtserkennung in der Strafverfolgung die richtige Kontrollinstitution ist. Wichtige Fragen wie die Fehleranfälligkeit dieser Maßnahme oder mögliche diskriminierende Wirkungen durch häufigere Fehlidentifizierungen bei einzelnen Bevölkerungsgruppen betreffen mehr als den – auf das Individuum zugeschnittenen – Datenschutz.[505] Aus kriminalpolitischer Sicht wird hier eine umfangreichere Kontrolle sinnvoll sein,[506] als verfassungsrechtlich zwingend hat das Bundesverfassungsgericht eine solche bislang, soweit ersichtlich, noch in keiner Konstellation angesehen (oder auch nur erörtert).

501 BVerfGE 65, 1 (46).

502 Kritisch zu dem vom Bundesverfassungsgericht häufig verwendeten Begriff „Aufsicht" *Schwabenbauer*, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, Kapitel G. Informationsverarbeitung im Polizei- und Strafverfahrensrecht, Rn. 294.

503 *Heckmann/Paschke*, in: Stern/Sodan/Möstl, Das Staatsrecht der Bundesrepublik Deutschland im europäischen Staatenverbund, 2. Aufl. 2022, § 103 Datenschutz, Rn. 47. Näher zur Datenschutzaufsicht im strafprozessualen Ermittlungsverfahren *Gisch*, KriPoZ 2020, 328.

504 Siehe etwa BVerfGE 133, 277 (365 f., 370 f.); 150, 244 (302); 155, 119 (227). Allerdings muss diese wirksam ausgestaltet sein, vgl. hierzu auch BVerfGE 141, 220 (321). Zu Art. 10 GG vgl. BVerfGE 100, 313 (361): „Wie die Kontrolle auszugestalten ist, schreibt die Verfassung jedoch nicht vor. Dem Gesetzgeber steht es frei, die ihm geeignet erscheinende Form zu wählen, wenn sie nur hinreichend wirksam ist."

505 In diese Richtung auch mit Blick auf personenbezogenes Predictive Policing *Sommerer*, Personenbezogenes Predictive Policing, 2020, 213. *Poscher* betont zutreffend, dass es in den Fällen der Festnahmen Unschuldiger nach falschen Gesichtserkennungstreffern weniger um ein formales Recht auf Datenschutz geht als um inhaltliche Recht wie das Recht auf Freiheit oder Schutz vor rassistischer Diskriminierung, vgl. *Poscher*, in: Vöneky/Kellmeyer/Müller/Burgard, The Cambridge Handbook of Responsible Artificial Intelligence, 2022, 281, 288 („The actual cases, however, are not about some formal right to data protection but about substantive rights, such as the right to liberty or the right against racial discrimination, and the dangers AI technologies pose for these rights.").

506 Hierzu Kapitel IV. C. II.

dd) Berichts- und Evaluationspflichten

Zudem stellt sich die Frage, ob Berichts- und Evaluationspflichten gegenüber Parlament und Öffentlichkeit verfassungsrechtlich geboten sind. In seiner Entscheidung zur Antiterrordatei im Jahr 2013 begründete das Bundesverfassungsgericht die Erforderlichkeit von Berichtspflichten für Speicherung und Nutzung der Daten nach dem Antiterrordateigesetz damit, dass sich diese der Wahrnehmung der Betroffenen und der Öffentlichkeit weitgehend entzögen, dass dem auch die Auskunftsrechte nur begrenzt entgegenwirken könnten und dass eine effektive gerichtliche Kontrolle nicht ausreichend möglich sei.[507] Diese Argumentation scheint auf andere heimliche Maßnahmen übertragbar, das Gericht sieht Berichtspflichten gegenüber Parlament und Öffentlichkeit aber nur in eng umgrenzten Fällen vor, etwa für „tief in die Privatsphäre eingreifende Ermittlungs- und Überwachungsbefugnisse mit spezifisch breitenwirksamem Grundrechtsgefährdungspotenzial".[508] Bei der automatisierten Kfz-Kennzeichenkontrolle wurde eine Berichtspflicht nicht einmal erörtert. Angesichts des zwar erheblichen, aber im Vergleich zu anderen heimlichen Maßnahmen nicht besonders erhöhten Eingriffsgewichts ist fraglich, ob das Bundesverfassungsgericht bei der Verwendung automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger Berichtspflichten annehmen wird. Angezeigt scheint dies aber durchaus. Jedenfalls aus kriminalpolitischer Perspektive sollten gerade bei einer so stark in der öffentlichen Diskussion stehenden Technologie wie der Gesichtserkennung Berichtspflichten geregelt werden; dies wird in Kapitel IV. erörtert.

Auch Pflichten zur Beobachtung und Evaluation des Einsatzes automatisierter Gesichtserkennung erscheinen sinnvoll. Das Bundesverfassungsgericht hat solche Pflichten bislang in unterschiedlichsten Rechtsgebieten etwa im Umweltrecht[509] und Versicherungsrecht[510] zwar vereinzelt angesprochen,[511] aber nicht näher ausgestaltet.[512] Im Bereich der Strafverfolgung

507 BVerfGE 133, 277 (273).
508 BVerfGE 155, 119 (228); vgl. auch BVerfGE 141, 220 (268 f., 285); BVerfGE 162, 1 (67 ff, 131 f.).
509 BVerfGE 49, 89 (130 ff.). Hierzu auch *Britz*, NVwZ 2023, 1449, 1457 mit Verweis auf weitere Entscheidungen.
510 BVerfG, NJW 2009, 2033 (2045).
511 Vgl. auch BVerfGE 150, 1 (90).
512 *Schwabenbauer*, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, Kapitel G. Informationsverarbeitung im Polizei- und Strafverfahrensrecht, Rn. 351.

und Gefahrenabwehr erscheint es angesichts des grundrechtssensiblen Einsatzbereichs und des raschen technologischen Fortschritts[513] besonders wichtig, Entwicklungen aufmerksam zu beobachten.[514] *Bäcker* weist zutreffend darauf hin, dass Effektivität und Eingriffsintensität einer Maßnahme etwa davon abhängen, „wie die Polizei die Maßnahme einsetzt, wie Kriminelle auf sie reagieren oder wie sich die Maßnahme auf Dritte auswirkt".[515] Zu dem Zeitpunkt, in dem der Gesetzgeber die Ermächtigungsgrundlage für eine Maßnahme schafft, sind solche Auswirkungen aber meist noch nicht absehbar.[516] Wie bereits im Abschnitt zum Gebot der Bestimmtheit und Normenklarheit angesprochen,[517] billigt das Bundesverfassungsgericht grundsätzlich eine „technikoffene" Formulierung der Maßnahmeermächtigungen. Im Gegenzug verlangt es aber vom Gesetzgeber „die technischen Entwicklungen aufmerksam [zu] beobachten und bei Fehlentwicklungen hinsichtlich der konkreten Ausfüllung offener Gesetzesbegriffe durch die Strafverfolgungsbehörden und die Strafgerichte notfalls durch ergänzende Rechtssetzung korrigierend ein[zu]greifen".[518] In seiner Entscheidung zum BKA-Gesetz betonte das Bundesverfassungsgericht mit Blick auf das Eingriffsgewicht einer Maßnahme, dass „der Gesetzgeber in seine Abwägung auch die Entwicklung der Informationstechnik einzustellen [habe], die die Reichweite von Überwachungsmaßnahmen zunehmend ausdehnt, ihre Durchführbarkeit erleichtert und Verknüpfungen erlaubt, die bis hin zur Erstellung von Persönlichkeitsprofilen reichen".[519] Diesen Äußerungen des Bundesverfassungsgerichts kann man zwar durchaus gewisse Beobachtungs- und Evaluationspflichten beim Einsatz neuer Technologien in Strafverfolgung und Gefahrenabwehr entnehmen. Näher konkretisiert und justiziabel gemacht wurden sie allerdings bislang nicht.

513 Vgl. auch BVerfGE 112, 304 (316) („[w]egen des schnellen und für den Grundrechtsschutz riskanten […] informationstechnischen Wandels").
514 Näher dazu, wie das Recht mit den technologischen Entwicklungen Schritt halten kann *Golla*, Kriminologisches Journal 2020, 149.
515 *Bäcker*, Kriminalpräventionsrecht, 2015, 181.
516 Vgl. *Bäcker*, Kriminalpräventionsrecht, 2015, 181; vgl. auch *Schwabenbauer*, Heimliche Grundrechtseingriffe, 2013, 358 ff.
517 Kapitel II. A. 3. b).
518 BVerfGE 112, 304 (316 f.); vgl. auch BVerfGE 90, 145 (191).
519 BVerfGE 141, 220 (267).

4. Fazit

Eine Rechtsgrundlage, auf die der Einsatz automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger gestützt werden soll, muss insbesondere verhältnismäßig sein und dem Gebot der Bestimmtheit und Normenklarheit genügen. Die Aufklärung von Straftaten ist ein legitimer Zweck; eine Beschränkung auf besonders schwere Straftaten ist nicht verfassungsrechtlich geboten. Als Ermächtigung für Eingriffe in das Recht auf informationelle Selbstbestimmung muss die Rechtsgrundlage Anlass, Zweck und Grenzen des Eingriffs bereichsspezifisch, präzise und normenklar regeln. Dabei sind wegen der erheblichen Eingriffsintensität erhöhte Anforderungen zu stellen. Auch sind Benachrichtigungspflichten vorzusehen. Eine wirksame Kontrolle ist ebenfalls erforderlich; die Ausgestaltung ist eine kriminalpolitische Frage.

Berichtspflichten für Parlament und Öffentlichkeit erscheinen durchaus angezeigt; ob das Bundesverfassungsgericht sie bei der Gesichtserkennung angesichts des „nur" erheblichen und nicht besonders erhöhten Eingriffsgewichts einfordern wird, ist hingegen fraglich. Auch Beobachtungs- und Evaluationspflichten wären zweckmäßig, sind bislang aber wenig justiziabel ausgestaltet.

II. Sonstige Grundrechte

Weiterhin ist zu fragen, ob neben dem Recht auf informationelle Selbstbestimmung auch andere Grundrechte beeinträchtigt werden und wie sich dies auf die Anforderungen an eine Rechtsgrundlage auswirkt. Dabei ist zum einen zu untersuchen, ob in bestimmten Konstellationen auch die Versammlungsfreiheit (Art. 8 Abs. 1 GG) betroffen ist. Zudem stellt sich die Frage, inwiefern der Einsatz automatisierter Gesichtserkennung mit gleichheitsrechtlichen Problemen (Art. 3 GG) einhergeht und ob die Menschenwürde betroffen ist.

1. Versammlungsfreiheit

Der Schutzbereich des Art. 8 Abs. 1 GG kann betroffen sein, wenn bei einer Versammlung Aufnahmen angefertigt werden und diese anschließend in ein Gesichtserkennungssystem eingespielt werden, um die Identität von

Personen zu ermitteln, die einer Straftat verdächtig sind. Dabei kann es sich um spezifisch versammlungsrechtliche Straftaten handeln (z. B. abweichende Durchführung von Versammlungen oder Verstöße gegen das Uniform- und politische Kennzeichenverbot, siehe für das Bundesversammlungsgesetz §§ 25, 28 VersG). In Betracht kommen aber auch andere Straftaten, die im Rahmen der Versammlung begangen werden, etwa Körperverletzungen, Beleidigungen oder Widerstand gegen Vollstreckungsbeamte. Dabei ist auch zu beachten, dass es im Versammlungskontext besonders schnell zum Verdacht einer Straftat kommen kann, etwa wenn Demonstranten ihre Meinung polemisch oder zugespitzt äußern und sie daher einer Beleidigung verdächtigt werden.

Art. 8 Abs. 1 GG ist neben dem Recht auf informationelle Selbstbestimmung anwendbar und wird nicht verdrängt.[520] Bereits die *Videoaufzeichnung* einer Versammlung durch Kameras,[521] Drohnen[522] oder Bodycams[523] stellt einen Eingriff in die Versammlungsfreiheit dar. Denn die Demonstranten können hierdurch von der Teilnahme abgeschreckt werden, was für einen Eingriff in die Versammlungsfreiheit ausreicht.[524] Die nun hinzukom-

520 Siehe nur OVG Nordrhein-Westfalen, DVBl 2011, 175; *Kniesel/Poscher*, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, Kapitel J. Versammlungsrecht, Rn. 190; *Poscher*, in: Gander/Perron/Poscher/Riescher/Würtenberger, Resilienz in der offenen Gesellschaft, 2012, 167; *Albers*, in: Friedewald/Lamla/Roßnagel, Informationelle Selbstbestimmung im digitalen Wandel, 11, 26 ff.; aA *Götz*, NVwZ 1990, 112, 116. Auch in BVerfGE 150, 244 (automatisierte Kennzeichenkontrolle) zieht das Bundesverfassungsgericht sowohl das Recht auf informationelle Selbstbestimmung als auch die Versammlungsfreiheit heran.

521 Vgl. nur BVerfGE 122, 342 (368 f.) (Eingriff bereits durch Übersichtsaufnahmen und -aufzeichnungen), siehe aus der Rechtsprechung etwa auch OVG Münster, Beschl. v. 23.11.2010, 5 A 2288/09, BeckRS 2010, 56136 und bereits OVG Bremen, NVwZ 1990, 1188, 1189; in der Literatur etwa Dreier GG/*Kaiser*, 4. Aufl. 2023, GG Art. 8 Rn. 51; *Heldt*, MMR 2019, 285, 288; *Koranyi/Singelnstein*, NJW 2011, 124. Ein Eingriff ist auch zu bejahen, wenn die Kameras nur im Kamera-Monitor laufen (also das Geschehen nicht aufzeichnen), vgl. etwa BVerfG, NVwZ 2009, 441 (447); dazu auch näher *Donaubauer*, Der polizeiliche Einsatz von Bodycams, 2017, 356 f., 360 ff. Siehe zudem BVerfGE 150, 244 (295) (Eingriff in Art. 8 GG durch den Einsatz automatisierter Kennzeichenkontrollen an Kontrollstellen, die den Zugang zu einer Versammlung kontrollieren).

522 Zur Verwendung von Video-Drohnen bei Versammlungen etwa *Tomerius*, LKV 2020, 481; *Zöller/Ihwas*, NVwZ 2014, 408; *Roggan*, NVwZ 2011, 590, 591.

523 Siehe nur *Martini/Thiessen/Ganter*, Digitale Versammlungsbeobachtung, 2023, 69 ff.

524 Siehe nur BVerwGE 160, 169 (182); vgl. auch BVerfGE 140, 225 (228); Dreier GG/*Kaiser*, 4. Aufl. 2023, GG Art. 8 Rn. 51; *Kloepfer*, in: Isensee/Kirchhof, Handbuch des Staatsrechts, Band VII, 3. Aufl. 2009, § 164 Rn. 74 („[s]pätestens dann, wenn durch

mende Möglichkeit, diese Aufzeichnungen anschließend per *Gesichtserkennung* auszuwerten,[525] könnte unter zwei Gesichtspunkten zu berücksichtigen sein.

a) Erhöhtes Eingriffsgewicht der Aufzeichnung der Versammlung

Zum einen erhöht sie die Eingriffsintensität des ursprünglichen Eingriffs in die Versammlungsfreiheit durch die Videoüberwachung. Denn durch die Möglichkeit der Gesichtserkennung läuft der Einzelne bei einer Videoaufzeichnung nicht nur Gefahr, aufgezeichnet zu werden, sondern danach noch identifiziert zu werden. Das Eingriffsgewicht einer Überwachungsmaßnahme im Zusammenhang mit der Versammlungsfreiheit bestimmt sich nach denselben Kriterien wie bei der informationellen Selbstbestimmung; eingriffserhöhend wirken auch hier insbesondere Heimlichkeit, Streubreite, Anlasslosigkeit, Erfassung höchstpersönlicher Merkmale, Möglichkeit der Verknüpfung.[526] Durch Gesichtserkennung werden besonders sensible Daten (biometrische Merkmale) verarbeitet und eine einfache Verknüpfung von Daten ermöglicht; dies erhöht den Eingriff erheblich. Daher sind an eine Rechtsgrundlage, die eine Videoüberwachung von Versammlungen erlaubt, erhöhte Anforderungen zu stellen, wenn die Aufnahmen danach zur Identifizierung Verdächtiger per Gesichtserkennung verwendet werden dürfen.

Dabei ist erneut (wie bereits beim Recht auf informationelle Selbstbestimmung[527]) darauf hinzuweisen, dass auch und gerade im Rahmen einer Versammlung eine *nachträgliche* Auswertung nicht per se weniger eingriffsintensiv ist als eine Echtzeit-Gesichtserkennung.[528] Gerade bei Ver-

staatliche Überwachungsmaßnahmen die innere Entschlußfreiheit des einzelnen Teilnehmers in der Weise so beschränkt wird, daß dieser aus Angst vor staatlichen Überwachungsmaßnahmen auf die ihm zustehende Grundrechtsausübung verzichtet").

525 Zu den hohen Anforderungen für eine Rechtfertigung beim Einsatz von Echtzeit-Gesichtserkennung *Martini/Thiessen/Ganter*, Digitale Versammlungsbeobachtung, 2023, 110 ff.

526 *Martini/Thiessen/Ganter*, Digitale Versammlungsbeobachtung, 2023, 57 ff.; *Schindler*, Biometrische Videoüberwachung, 2021, 472. Zu den Kriterien bereits Kapitel II. A. I. 2. b).

527 Kapitel II. A. I. 2. b) hh).

528 *Hahn*, ZfDR 2023, 142, 155 ff. In eine ähnliche Richtung (allerdings nicht im Versammlungskontext) *Rostalski/Weiss*, in: Hilgendorf/Roth-Isigkeit, Die neue Verord-

sammlungen können eine nachträgliche Gesichtserkennung und damit verzögerte Maßnahmen der Strafverfolgungsbehörden sogar problematischer sein, denn sie können eine große Verunsicherung auslösen und geschehen außerhalb der mit einer Versammlung oft einhergehenden medialen Kontrolle des polizeilichen Handelns.[529] Erinnert sei nur an die Praktiken Russlands, Hunderte Demonstranten nach der Teilnahme an Versammlungen zu Hause festzunehmen – nachträglich identifiziert per Gesichtserkennung.[530] Natalia Zviagina, die Leiterin des Moskau-Büros von Amnesty International, sagte dazu: „Bisher bestand das größte Risiko für die Demonstranten darin, bei einer Kundgebung von der Polizei verprügelt und willkürlich festgenommen zu werden. Diesem Schicksal zu entgehen, bedeutet ab sofort nicht mehr, dass man sich sicher fühlen kann – der Unterdrückungsstaat weiß, wer man ist, und kann einen jederzeit abholen."[531] Deutschland ist nicht Russland, aber die Äußerung trifft den Kern. Bei einer Echtzeit-Gesichtserkennung weiß der Betroffene nach Verlassen der Versammlung, dass ihm nun nichts mehr droht. Er hat zumindest Gewissheit. Bei einer nachträglichen Auswertung bleibt die Unsicherheit bestehen – noch Tage, Wochen und Monate später. Außerdem werden Festnahmen

---

nung der EU zur Künstlichen Intelligenz, 2023, 35 (44); *Linardatos*, GPR 2022, 58 (62); *Schindler/Schomberg*, in: Friedewald/Roßnagel/Heesen/Krämer/Lamla, Künstliche Intelligenz, Demokratie und Privatheit, 2022, 103 (121); *Rostalski/Weiss*, ZfDR 2021, 329, 344. Anders *Martini/Thiessen/Ganter*, Digitale Versammlungsbeobachtung, 2023, 111 f., die argumentieren, dass eine „Live-Auswertung anhand biometrischer Merkmale […] spürbar größeres Eingriffspotenzial [berge] als eine Ex-post-Analyse von Fotos und Videoaufnahmen. Denn eine Echtzeitanalyse ermöglicht es den überwachenden Beamten, unmittelbar Vollzugsmaßnahmen zu ergreifen. Sie können identifizierte Personen direkt aus der Versammlung heraus aufgreifen sowie ggf. festnehmen und müssen diese – anders als bei einer Ex-post-Auswertung – nicht erst zur Fahndung ausschreiben. Für Versammlungsteilnehmer hat dies zur Folge, dass sie bereits während einer Versammlung mit der Aufhebung ihrer Anonymität und den daraus folgenden Maßnahmen rechnen müssen." Dem ist insofern zuzustimmen, dass die Echtzeit-Gesichtserkennung einen spürbaren Eingriff in die Versammlungsfreiheit darstellt. Das gilt aber ebenso für die Erkennung im Nachhinein. Darauf, dass auch die nachträgliche Gesichtserkennung einen erheblichen Eingriff bedeutet, weisen aber auch *Martini/Thiessen/Ganter*, Digitale Versammlungsbeobachtung, 2023, 112 hin.

529 *Hahn*, ZfDR 2023, 142, 157.

530 Hierzu bereits Kapitel I G. II. 1. c).

531 *Amnesty International*, News v. 27.4.2021, https://perma.cc/9G8D-CG8B („Previously the protesters' main risk was being beaten and arbitrarily detained by police at a rally. As of now, avoiding this fate does not mean that you can feel safe – the repressive state knows who you are and can come for you at any point.").

bei einer Versammlung regelmäßig auch von der Presse dokumentiert und in der Bevölkerung wahrgenommen; spätere Maßnahmen der Behörden bleiben der Öffentlichkeit dagegen verborgen. Eine nachträgliche Auswertung von Aufzeichnungen einer Versammlung per Gesichtserkennung ist daher nicht per se weniger eingriffsintensiv als eine Echtzeit-Auswertung.

Die Videoüberwachung einer Versammlung hat daher eine höhere Eingriffsintensität, wenn die Aufzeichnungen zur Gesichtserkennung (auch im Nachhinein) verwendet werden können. Dies müsste bei den versammlungsrechtlichen Ermächtigungsgrundlagen[532] für den Einsatz von Videoüberwachung, Drohnen und Body-Cams berücksichtigt werden.[533]

b) Berücksichtigung der Versammlungsfreiheit bei späterer Gesichtserkennung

Zum anderen stellt sich die Frage, ob und wie die Versammlungsfreiheit bei der anschließenden Auswertung der Videoaufnahmen einer Versammlung zur Identifizierung unbekannter Verdächtiger zu berücksichtigen ist. Insbesondere ist zu fragen, ob die Identifizierung einen erneuten Eingriff in die Versammlungsfreiheit darstellt.[534] Da ein Eingriff in die Versammlungsfrei-

532 Wegen der Polizeifestigkeit des Versammlungsrechts (hierzu etwa BVerwGE 129, 142 (147); *Voßkuhle/Schemmel*, JuS 2022, 1113, 1116; *Kniesel/Poscher*, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, Kapitel J. Versammlungsrecht, Rn. 24 ff.; *Friedrich*, DÖV 2019, 55, 57; *Hoffmann-Riem*, in: Merten/Papier, Handbuch der Grundrechte, Bd. IV, 2011, § 106 Rn. 14, 19, 22; *Kötter/Nolte*, DÖV 2009, 399, 402 ff.) müssen diese Maßnahmen in dem jeweiligen Versammlungsgesetz geregelt sein. Die bisherigen Regelungen in den Versammlungsgesetzen halten keine Rechtsgrundlage für die Echtzeit-Auswertung von Videoaufzeichnungen im Rahmen einer Versammlung bereit, *Martini/Thiessen/Ganter*, Digitale Versammlungsbeobachtung, 2023, 94 ff.

533 Zu den Anforderungen an eine solche Ermächtigungsgrundlage vgl. *Martini/Thiessen/Ganter*, Digitale Versammlungsbeobachtung, 2023, 99 f., die sich damit aber offenbar nur auf Echtzeit-Gesichtserkennung beziehen, wenn sie für die nachträgliche Auswertung ausschließlich von einer Eingriffsermächtigung in der StPO sprechen. Die Möglichkeit der nachträglichen Auswertung (auf Basis einer Rechtsgrundlage in der StPO) sollte aber auch bei der Eingriffsintensität für den ursprünglichen Eingriff in die Versammlungsfreiheit eingriffserhöhend berücksichtigt werden.

534 So wohl *Martini/Thiessen/Ganter*, Digitale Versammlungsbeobachtung, 2023, 112, die davon sprechen, dass eine Ex-post-Gesichtserkennung einen schwerwiegenden Eingriff in die Versammlungsfreiheit auslöst; einen Eingriff in Art. 8 GG bejaht auch *Schindler*, Biometrische Videoüberwachung, 2021, 349 mit der Begründung, dass das Bundesverfassungsgericht davon ausgeht, dass bei Daten, die durch Eingriff in

heit bereits bejaht wird, wenn Bürger davon abgeschreckt werden könnten, an einer Versammlung teilzunehmen, ließe sich argumentieren, dass eine nachträgliche Erkennung die Versammlungsfreiheit insofern beschränkt, dass die Bürger zukünftige Versammlungen nun meiden. Allerdings ist fraglich, ob Art. 8 GG zum Zeitpunkt der (nachträglichen) Identifizierung Verdächtiger überhaupt noch zeitlich anwendbar ist.[535] Die Versammlungsfreiheit schützt vor allem die eigentliche Versammlungsdurchführung; sie gewährt aber auch einen Vorfeldschutz, etwa mit Blick auf die Ankündigung der Veranstaltung, Teilnahmeaufrufe, die Anreise und den Zugang zur Versammlung.[536] Denn andernfalls liefe die Versammlungsfreiheit Gefahr, durch staatliche Maßnahmen im Vorfeld der Grundrechtsausübung ausgehöhlt zu werden.[537] Auch in der Beendigungsphase wirkt Art. 8 GG fort, das freie, geordnete Verlassen des Versammlungsorts muss für die Teilnehmer möglich sein,[538] da Personen andernfalls von der Teilnahme an zukünftigen Versammlungen abgehalten werden könnten.[539] Ob dies allerdings noch weit im Nachgang an eine Versammlung für die Auswertung von Bildmaterial gilt, ist fraglich.

Art. 10 Abs. 1 GG und Art. 13 Abs. 1 GG erhoben wurden, auch deren Folgeverwendung an diesen Grundrechten zu messen ist; diese Argumentation sei auf Art. 8 GG übertragbar. Zu dieser Rechtsprechung des Bundesverfassungsgerichts siehe BVerfGE 100, 313 (359); 110, 33 (68 f.); 113, 348 (365); 125, 260 (313); 133, 277 (317).

535 Auch müsste man fragen, ob (nur) die Auswertung als solche eine faktische Behinderung von einem solchen Gewicht ist, dass sie einer imperativen Maßnahme gleichkommt (und daher einen eigenständigen Eingriff begründet).

536 Dürig/Herzog/Scholz/*Depenheuer*, 102. EL August 2023, GG Art. 8 Rn. 80; BeckOK GG/*Schneider*, 56. Ed., Stand: 15.8.2023, GG Art. 8 Rn. 21; *Kloepfer*, in: Isensee/Kirchhof, Handbuch des Staatsrechts, Band VII, 3. Aufl. 2009, § 164 Rn. 45; ausführlich *Ebeling*, Die organisierte Versammlung, 2017, 231 ff.

537 BVerfGE 69, 315 (349); 84, 203 (209); siehe auch BVerwG, NJW 2018, 716 (720);

538 So VG Hamburg, NVwZ 1987, 829, 833: „Die Versammlungsfreiheit schützt das freie Zusammenströmen, die eigentliche Versammlung und das freie Auseinanderströmen der Teilnehmer gleichermaßen.". Siehe auch v. Münch/Kunig/*Ernst*, 7. Aufl. 2021, GG Art. 8 Rn. 70 mit Verweis auf die frühere gegenteilige Auffassung in der Rechtsprechung.

539 VG Hamburg, NVwZ 1987, 829 (833); v. Münch/Kunig/*Ernst*, 7. Aufl. 2021, GG Art. 8 Rn. 70; Sachs/*Höfling*, 9. Aufl. 2021, GG Art. 8 Rn. 26 (mit der Einschränkung auf „[s]taatliche Maßnahmen im Anschluss an die Versammlung, welche darauf abzielen, von der künftigen Teilnahme an Versammlungen abzuhalten").

Ungeachtet der Frage, ob man hierin einen eigenständigen Eingriff sehen will, kommt aber jedenfalls der objektiv-rechtliche Gehalt[540] der Versammlungsfreiheit hier weiterhin zum Tragen. Die Grundrechte sind nicht nur Abwehrrechte, sondern auch eine grundlegende verfassungsrechtliche Wertentscheidung; sie entfalten daher Ausstrahlungswirkungen auf die gesamte Rechtsordnung. Die Versammlungsfreiheit ist für eine freiheitlich demokratische Staatsordnung konstituierend[541] und gewährleistet, so das Bundesverfassungsgericht, „ein Stück ursprünglicher ungebändigter unmittelbarer Demokratie“[542]. Diese hohe Bedeutung des Art. 8 GG ist bei der Auslegung von Rechtsvorschriften zu beachten.[543] Das Gebot einer versammlungsfreundlichen Auslegung gilt nicht nur für versammlungsrechtliche Vorschriften, sondern erstreckt sich darüber hinaus auf alle Rechtsbereiche,[544] gilt also etwa auch für straf- und haftungsrechtliche Maßnahmen nach einer Versammlung.[545] Der BGH hat die Versammlungsfreiheit in einer strafrechtlichen Entscheidung etwa dahingehend berücksichtigt, dass eine Mittäterschaft oder Beihilfe an gewalttätigen Ausschreitungen im Rahmen einer Versammlung nicht vorschnell angenommen werden darf.[546] Daher lässt sich argumentieren, dass auch eine Rechtsgrundlage, auf die eine Identifizierung von Versammlungsteilnehmern wegen (mut-

540 Näher hierzu mit Blick auf die Versammlungsfreiheit etwa Sachs/*Höfling*, 9. Aufl. 2021, GG Art. 8 Rn. 47 ff. Zu den Grundrechten als objektiv-rechtliche Wertentscheidungen auch BVerfGE 39, 1 (41); 88, 203 (251).

541 BVerfGE 128, 226 (250); zur hohen Bedeutung der Versammlungsfreiheit etwa auch *Kloepfer*, in: Isensee/Kirchhof, Handbuch des Staatsrechts, Band VII, 3. Aufl. 2009, § 164 Rn. 1.

542 BVerfGE 69, 315 (347) unter Verweis auf *Hesse*, Grundzüge des Verfassungsrechts, 20. Aufl. 1999, Rn. 404.

543 Siehe nur BVerfGE 69, 315 (348 f.); 87, 399 (407); vgl. etwa auch BVerfG, NVwZ 2007, 1180, 1182; *Hufen*, Staatsrecht II Grundrechte, 10. Aufl., 2023, § 30 Versammlungsfreiheit Rn. 23; *Voßkuhle/Schemmel*, JuS 2022, 1113, 1115; Jarass/Pieroth/*Jarass*, 17. Aufl. 2022, GG Art. 8 Rn. 19; *Koranyi/Singelnstein*, NJW 2011, 124.

544 Huber/Voßkuhle/*Gusy*, 8. Aufl. 2024, GG Art. 8 Rn. 46.

545 BVerfGE 69, 315, (361 f.).

546 Siehe BGH, NJW 1984, 1226, 1229, wonach es wegen der Wertungen des Art. 8 GG für die Annahme einer Mittäterschaft oder Beihilfe an gewalttätigen Ausschreitungen bei einer Versammlung nicht schon ausreicht, dass „der an ihnen nicht aktiv beteiligte Demonstrant an Ort und Stelle verharrt, auch wenn er, wie es die Regel sein wird, von vornherein mit Gewalttätigkeiten einzelner oder ganzer Gruppen rechnet und weiß, daß er allein schon mit seiner Anwesenheit den Gewalttätern mindestens durch Gewährung von Anonymität Förderung und Schutz geben kann“. Denn ein solches Verhalten könne auch nur die Kundgabe der eigenen Meinung zu den sachlichen Anliegen der Demonstration in der Öffentlichkeit darstellen.

maßlicher) Straftaten gestützt wird, im Lichte der besonderen Bedeutung der Versammlungsfreiheit auszulegen ist.[547] Das könnte bedeuten, eine Identifizierung nur zur Aufklärung von Straftaten einer bestimmten Schwere zuzulassen.[548] Dann muss die Rechtsgrundlage aber überhaupt in dieser Hinsicht einer Auslegung zugänglich sein. Es sei aber bereits hier vorab darauf verwiesen, dass dies bei den strafprozessualen Normen, die für eine Gesichtserkennung herangezogen werden könnten (insbesondere § 98c StPO), nicht der Fall ist. Davon abgesehen wäre es möglich, den besonderen Versammlungskontext bei der Auswertung der Aufnahmen zur Identifizierung unbekannter Verdächtiger bereits ausdrücklich in der strafprozessualen Ermächtigungsgrundlage zu berücksichtigen.[549]

2. Diskriminierungsverbot

Zudem kann der Einsatz von Gesichtserkennung in der Strafverfolgung gleichheitsrechtliche Fragen aufwerfen.[550] Viele Gesichtserkennungsalgorithmen haben erheblich höhere Fehlerraten für einige Gruppen, etwa People of Color oder Frauen.[551] Das kann dazu führen, dass diese Menschen auch deutlich häufiger unschuldig[552] Ermittlungsmaßnahmen ausgesetzt sind. Daher steht eine Ungleichbehandlung im Raum, insbesondere ist

547 Vgl. auch BVerfG, NVwZ 2017, 555 zu Maßnahmen nach § 163b StPO und § 163c StPO im Rahmen einer Versammlung.

548 In diese Richtung wohl auch *Martini/Thiessen/Ganter*, Digitale Versammlungsbeobachtung, 2023, 112; vgl. auch *United Nations High Commissioner for Human Rights*, Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests, Report, UN Doc. A/HRC/44/24, 2020, 10.

549 Hierzu Kapitel IV. B. III.

550 Siehe auch *Schindler*, Biometrische Videoüberwachung, 2021, 655; kurze Erwähnung bei *Golla*, in: Chibanguza/Kuß/Steege, Künstliche Intelligenz, 2022, 2. Teil: § 9 A. KI-Einsatz bei der Polizei Rn. 18 f. und *Hornung/Schindler*, DuD 2021, 515, 517. Zu Fragen der Diskriminierung durch algorithmische Systeme siehe etwa BeckOK GG/*Kischel*, Art. 3 Abs. 3 Rn. 218a ff.; *Lauscher/Legner*, ZfDR 2022, 367; *Müller*, in: BMUV/Rostalski, Künstliche Intelligenz, 2022, 205; *von Ungern-Sternberg*, in: Vöneky/Kellmeyer/Müller/Burgard, The Cambridge Handbook of Responsible Artificial Intelligence, 2022, 252; *von Ungern-Sternberg*, in: Mangold/Payandeh, Handbuch Antidiskriminierungsrecht, 2022, 1131; *Härtel* LKV 2019, 49, 56 f.; *Heldt*, MMR 2019, 285, 286; *Steege,* MMR 2019, 715; *Martini*, JZ 2017, 1017, 1018 f.

551 Kapitel I. E. IV. 5.

552 Wie bereits angesprochen, ist damit gemeint: ohne dass sich der Tatvorwurf im Nachgang bestätigen lässt.

zu fragen, ob Art. 3 Abs. 3 GG verletzt wird. Eine unmittelbare Benachteiligung scheidet aus, da beim Einsatz von Gesichtserkennung nicht ausdrücklich an verbotene Merkmale wie Geschlecht oder „Rasse“[553] angeknüpft wird.[554] In Betracht kommt nur eine mittelbare Benachteiligung.[555] Eine solche liegt vor, wenn nicht direkt an eines der Merkmale angeknüpft wird, sondern sich die Diskriminierung aus den tatsächlichen Auswirkungen einer Regelung ergibt.[556] Dabei ist danach zu fragen, ob faktisch weitgehend nur eine Gruppe benachteiligt wird, deren Ungleichbehandlung nach Art. 3 Abs. 3 GG strikt verboten ist. Eine Diskriminierungsabsicht oder auch nur Kenntnis (der handelnden Person) von den diskriminierenden Wirkungen ist nicht erforderlich.[557] Es genügt, dass sich eine Maßnahme zum Nachteil einer durch die verbotenen Merkmale geschützten Gruppe auswirkt. Erfasst sind nicht nur rechtliche, sondern auch tatsächliche Benachteiligungen.[558] Die Figur der mittelbaren Benachteiligung ist als solche und im Einzelnen umstritten[559] und in der Rechtsprechung noch nicht ausreichend

553 Hierzu wird auch die Hautfarbe gezählt, siehe etwa Dürig/Herzog/Scholz/*Langenfeld*, 102. EL August 2023, GG Art. 3 Abs. 3 Rn. 45; dazu kritisch Dreier GG/*von Achenbach*, 4. Aufl. 2023, GG Art. 3 Abs. 2 Rn. 82 („schreibt das biologische Fehlverständnis von unterscheidbaren ‚Menschenrassen‘ unvermeidlich fort“). Kritisch zum Begriff „Rasse“ etwa *Kutting/Amin*, DÖV 2020, 612, 613 f.; *Ludyga,* NJW 2021, 911.

554 Instruktiv zu unterschiedlichen Gleichheitskonzeptionen hinter den Verboten der unmittelbaren und der mittelbaren Diskriminierung *Sacksofsky*, in: Mangold/Payandeh, Handbuch Antidiskriminierungsrecht, 2022, 597, 603 ff. Rn. 15 ff.

555 Teilweise wird auch von „faktischer Benachteiligung“ (z. B. BVerfGE 113, 1 (20)) oder „indirekter Ungleichbehandlung“ (z. B. Jarass/Pieroth/*Jarass*, 17. Aufl. 2022, GG Art. 3 Rn. 137) gesprochen.

556 Vgl. nur BVerfGE 113, 1 (15); 121, 241 (254 f.).

557 *Sacksofsky*, in: Mangold/Payandeh, Handbuch Antidiskriminierungsrecht, 2022, 597, 634 Rn. 108. Anders wohl *Schindler*, Biometrische Videoüberwachung, 2021, 665, der im Kontext der Gesichtserkennung scheinbar (auch) darauf abstellt, ob die Unterschiede in der Erkennungsleistung „intendiert“ sind.

558 Siehe nur Huber/Voßkuhle/*Baer/Markard*, 8. Aufl. 2024, GG Art. 3 Rn. 421.

559 Auf die Figur der mittelbaren Benachteiligung greift das Bundesverfassungsgericht bislang mit Blick auf Ungleichbehandlungen wegen des Geschlechts zurück, siehe etwa BVerfGE 113, 1 (15); 121, 241 (254 f.); 126, 29 (53); siehe jüngst aber auch BVerfGE 160, 79 (112) zu mittelbarer Benachteiligung wegen Behinderung; die Figur der mittelbaren Benachteiligung bejahend Dreier GG/*von Achenbach*, 4. Aufl. 2023, GG Art. 3 Abs. 2 Rn. 41; Jarass/Pieroth/*Jarass*, 17. Aufl. 2022, GG Art. 3 Rn. 137; Sachs/*Nußberger*, 9. Aufl. 2021, GG Art. 3 Rn. 248 ff.; Huber/Voßkuhle/*Baer/Markard*, 8. Aufl. 2024, GG Art. 3 Rn. 429; ablehnend zur Rechtsfigur der mittelbaren Diskriminierung *Sachs* in: Isensee/Kirchhof, Handbuch des Staatsrechts, Band VIII § 182 Rn. 32; differenzierend (nur für Geschlecht) BeckOK GG/*Kischel*,

konkretisiert worden. Mit Blick auf eine mittelbare Ungleichbehandlung durch den Einsatz von Gesichtserkennung und höhere Fehlerraten für einzelne Gruppen stellen sich mehrere Fragen und Probleme:

Erstens ist fraglich, auf welche „Auswirkungen" für die Feststellung einer Ungleichbehandlung abzustellen ist: auf möglicherweise erhöhte Fehlerraten eines Gesichtserkennungssystems für bestimmte Gruppen oder auf möglicherweise häufigere Ermittlungsmaßnahmen gegen Angehörige einer Gruppe, bei denen sich hinterher die Unschuld herausstellt. Für ein Abstellen bereits auf erhöhte Fehlerraten spricht, dass bereits mit einer Fehl-Erkennung die Gefahr einhergeht, Ermittlungsmaßnahmen ausgesetzt zu sein. Bereits dieses erhöhte Risiko könnte man als einen Nachteil begreifen. Dagegen lässt sich jedoch argumentieren, dass ein (falscher) Treffer noch nicht bedeutet, dass gegen diese Person tatsächlich ermittelt wird; zunächst muss ein Mensch den Treffer als richtig bestätigen und die Entscheidung treffen, dass nun weitere Maßnahmen ergriffen werden. Eine Ungleichbehandlung stellt es aber jedenfalls dar, wenn gegen Angehörige bestimmter Personengruppen nach Gesichtserkennungstreffern häufiger ermittelt wird, obwohl sich im Nachhinein herausstellt, dass sie unschuldig waren.[560] Denn jedenfalls dann hätten die fehlerhaften Erkennungen handfeste nachteilige Auswirkungen.

Zweitens stellt sich dann aber die Frage, wie stark ungleich die Auswirkungen sein müssen, um eine Ungleichbehandlung anzunehmen.[561] Ist es

---

56. Ed., Stand: 15.8.2023, GG Art. 3 Rn. 215. Die Rechtsfigur basiert auf dem vom US-amerikanischen Supreme Court entwickelten Konzept des „disparate impact", das in Griggs v. Duke Power Co., 401 US 424, 432 (1971) entwickelt wurde.

560 In diese Richtung auch *von Ungern-Sternberg*, in: Mangold/Payandeh, Handbuch Antidiskriminierungsrecht, 2022, 1131, 1143 Rn. 24: „Wenn Fehler bei der Gesichtserkennung etwa überwiegend zur Verhaftung falscher dunkelhäutiger Personen führen, lässt sich dies durchaus als Benachteiligung im diskriminierungsrechtlichen Sinn einstufen." Nicht ganz eindeutig bei *Schindler*, Biometrische Videoüberwachung, 2021, 665, der einerseits zutreffend darauf hinweist, dass „Unterschiede in der Erkennungsleistung bei unterschiedlichen Personengruppen […] dazu führen [können], dass Mitglieder einer Gruppe häufiger Fehlerkennungen und Verwechslungen ausgesetzt sind als Mitglieder anderer Gruppen, was sich wiederum in Gestalt zusätzlicher belastender Maßnahmen (z. B. Anhalten zur Identitätsfeststellung) äußern kann", andererseits aber auf die „Unterschiede in der Erkennungsleistung" (der Gesichtserkennungssysteme) abstellt. Ebenfalls nicht ganz eindeutig bei *Hornung/Schindler*, DuD 2021, 515, 517, die davon sprechen, dass es „zu gleichheitsrechtlichen Problemen kommen kann, wenn die Algorithmen bestimmte Bevölkerungsgruppen besser oder schlechter erkennen".

561 Vgl. auch *Schindler*, Biometrische Videoüberwachung, 2021, 665.

eine Ungleichbehandlung, wenn sich in 1000 Fällen herausstellt, dass die falsche Person als Verdächtiger identifiziert wurde und es sich dabei in 300 Fällen um People of Color handelt?[562] Dabei müsste aber auch berücksichtigt werden, wie viel Prozent der Ermittlungsverfahren insgesamt gegen Personen dieser Gruppe geführt werden. Wenn in dem Beispiel nur 350 Verfahren insgesamt gegen People of Color geführt wurden, dann ist eine „Quote" von 300 Ermittlungen gegen Unschuldige sehr hoch. Aussagekräftiger wäre es, für verschiedene Gruppen (z. B. Männer, Frauen, People of Color, Weiße) zu ermitteln, in wie viel Prozent aller Ermittlungsverfahren gegen diese Gruppe im Zusammenhang mit Gesichtserkennung am Ende sich herausstellte, dass gegen den falschen Verdächtigen ermittelt wurde. Wenn etwa (fiktiv) in 1000 Fällen gegen Männer ermittelt wurde, davon in 20 Verfahren gegen einen Unschuldigen (2 %), hingegen insgesamt in 100 Fällen gegen Frauen ermittelt wurde, davon in 15 Verfahren gegen Unschuldige (15 %), dann spräche dies dafür, dass Gesichtserkennung Frauen benachteiligt.[563]

Drittens zeigt sich dadurch auch ein weiteres, und zwar das größte Problem: die Nachweisbarkeit.[564] Die Fälle von Ermittlungen nach Gesichtserkennungstreffern müssten ausführlich dokumentiert und ausgewertet werden, auch anhand der oben genannten Kriterien. Diese Informationen müssten zudem den Betroffenen in allgemeinverständlicher Sprache zur Verfügung stehen. Eine solche Evaluierung findet aber, soweit ersichtlich, nicht statt; die Fälle werden nicht einmal unabhängig von der Frage möglicher Diskriminierungen systematisch näher nachverfolgt.[565]

562 Die Frage, was Fairness ist, stellt sich auch im Zusammenhang mit anderen algorithmischen Anwendungen, siehe etwa zum Widerstreit verschiedener Gleichheitsmaße beim Predictive Policing *Sommerer*, Personenbezogenes Predictive Policing, 2020, 184 ff.; siehe auch *Zweig/Krafft*, in: Mohabbat Kar/Thapa/Parycek, (Un)Berechenbar? Algorithmen und Automatisierung in Staat und Gesellschaft, 2018, 204 ff.

563 Um die Intersektionalität von Diskriminierung abzubilden, müsste zudem noch näher differenziert werden, etwa nach weiblichen People of Color (höchste Fehlerrate bei vielen Gesichtserkennungssystemen), männlichen People of Color, weißen Frauen, weißen Männern etc. Zudem müsste auch innerhalb der People of Color noch näher differenziert werden.

564 Vgl. im Übrigen zu den Durchsetzungsproblemen im Antidiskriminierungsrecht *Wachter/Mittelstadt/Russell*, Computer Law & Security Review 2021, 105567; *Orwat*, Diskriminierungsrisiken durch Verwendung von Algorithmen, 2019, 107 f.; *Hacker*, Common Market Law Review 2018, 1143, 1167 ff.

565 Kapitel I. F. I. 5.

Ob der Einsatz automatisierter Gesichtserkennung und die daraus folgenden weiteren Ermittlungen eine mittelbare Diskriminierung darstellen, kann also nicht pauschal beantwortet werden.[566] Deutlich wird hierbei erneut, dass – ungeachtet der Frage einer verfassungsrechtlichen Pflicht – eine Evaluierung der verwendeten Gesichtserkennungssysteme sowie der aus ihrer Anwendung folgenden polizeilichen Ermittlungspraxis dringend nötig ist.

3. Menschenwürde

Nicht zuletzt stellt sich auch die Frage, inwiefern die Menschenwürde Grenzen für den Einsatz automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger setzt. Das Bundesverfassungsgericht konkretisiert die Menschenwürde ex negativo vom Eingriff her.[567] Ob sie verletzt sei, könne nicht abstrakt bestimmt werden, „sondern immer nur in Ansehung des konkreten Falles".[568] Dabei greift das Bundesverfassungsgericht auf die „Objektformel"[569] zurück, wonach es der menschlichen Würde widerspricht, „den Menschen zum bloßen Objekt im Staat zu machen".[570] Für den Bereich der Datenverarbeitung durch den Staat statuierte das Gericht bereits 1969 im Mikrozensus-Beschluss, dass es mit der Menschenwürde nicht zu vereinbaren wäre, wenn der Staat das Recht für sich in Anspruch nehmen könnte, „den Menschen zwangsweise in

566 So im Ergebnis auch *Schindler*, Biometrische Videoüberwachung, 2021, 665. Welche Maßstäbe für eine Rechtfertigung mittelbarer Benachteiligung anzulegen sind, ist in der verfassungsgerichtlichen Rechtsprechung noch nicht geklärt, hierzu näher *Sacksofsky*, in: Mangold/Payandeh, Handbuch Antidiskriminierungsrecht, 2022, 597, 641 Rn. 135 f. Im Zusammenhang mit dem Einsatz von Gesichtserkennung dürfte eine Rechtfertigung allerdings schwerfallen, so auch *Schindler*, Biometrische Videoüberwachung, 2021, 666.

567 *Dreier,* Idee und Gestalt des freiheitlichen Verfassungsstaates, 2014, 90. Zu Vorschlägen für eine mögliche positive Bestimmung der Menschenwürde siehe etwa *Hillgruber*, in: Stern/Sodan/Möstl, Das Staatsrecht der Bundesrepublik Deutschland im europäischen Staatenverbund, 2. Aufl. 2022, § 100 Schutz der Menschenwürde, Rn. 17 ff.; v. Münch/Kunig/*Kunig/Kotzur*, 7. Aufl. 2021, GG Art. 1 Rn. 31 f.

568 BVerfGE 30, 1 (25); 115, 118 (153).

569 Kritik an der „Objektformel" etwa bei *Herdegen*, JZ 2001, 773 775; *Hilgendorf*, Jahrbuch für Recht und Ethik 1999, 137, 141 ff.; siehe auch v. Münch/Kunig/*Kunig/Kotzur*, 7. Aufl. 2021, GG Art. 1 Rn. 34 mwN.

570 BVerfGE 27, 1 (6); stRspr. Zuvor bereits *Dürig*, AöR 1956, 117, 127; ähnlich *Wintrich*, Zur Problematik der Grundrechte, 1957, 7.

seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren […] und ihn damit wie eine Sache zu behandeln, die einer Bestandsaufnahme in jeder Beziehung zugänglich ist".[571] In eine ähnliche Richtung – freilich nicht spezifisch zur Menschenwürde im Sinne des Grundgesetzes – geht auch die Formulierung der von der EU-Kommission eingesetzten unabhängigen High Level Expert Group on Artificial Intelligence: „Im Kontext der KI gebietet es die Achtung der Würde des Menschen, dass alle Menschen mit Respekt zu behandeln sind, da es sich um moralische Subjekte und nicht um bloße Objekte handelt, die es zu sieben, zu sortieren, zu bewerten, zu gruppieren, zu konditionieren oder zu manipulieren gilt."[572]

Speziell im Hinblick auf den Einsatz neuer Technologien im Sicherheitsrecht ist vor allem an das Verbot einer „Rundumüberwachung" zu denken,[573] mit der ein umfassendes Persönlichkeitsprofil[574] erstellt werden könnte. Danach ist es mit der Menschenwürde unvereinbar, wenn staatliche Überwachungsmaßnahmen sich über einen längeren Zeitraum erstrecken und derart umfassend sind, dass nahezu lückenlos alle Bewegungen und Lebensäußerungen des Betroffenen registriert werden und zur Grundlage

571 BVerfGE 27, 1 (6). Vgl. auch allgemein zur zunehmenden Menschenwürderelevanz des Datenschutzrechts *Hilgendorf*, Zeitschrift für Evangelische Ethik 2013, 258, 269; in eine ähnliche Richtung *Gusy/Eichenhofer*, in: FS Vedder 2017, 132, 144 unter Verweis auf *von Lewinski*, Die Matrix des Datenschutzes, 2014, 19.

572 *High Level Expert Group on Artificial Intelligence*, Ethics guidelines for trustworthy AI, 8.4.2019, 13. Die Expertengruppe versteht Menschenwürde in diesem Zusammenhang weniger im Sinne der Objektformel, sondern vielmehr als einen normativen Anker, auf den sich (fast) alle Mitglieder einer Gesellschaft einigen können; siehe zu dieser Konzeption der Menschenwürde *Hilgendorf*, in: Grimm/Kemmerer/Möllers, Human Dignity in Context, 2018, 325; *Hilgendorf*, Zeitschrift für Evangelische Ethik 2013, 258, insbesondere 269: „Wie müssen wir ‚Menschenwürde' konzipieren, um die von uns damit verfolgten Ziele erreichen zu können?".

573 BVerfGE 109, 279 (323); 112, 304 (319); vgl. auch BVerfGE 65, 1 (43). Das Bundesverfassungsgericht scheint die Rundumüberwachung als eigenständigen Verstoß gegen die Menschenwürde anzusehen statt als Verletzung des Menschenwürdekerns des Rechts auf informationelle Selbstbestimmung; hierzu auch Huber/Voßkuhle/*Eichberger*, 8. Aufl. 2024, GG Art. 2 Rn. 315. Zum Verbot der Rundumüberwachung siehe auch *Schwabenbauer*, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, Kapitel G. Informationsverarbeitung im Polizei- und Strafverfahrensrecht, Rn. 171; *Papier*, in: Merten/Papier, Handbuch der Grundrechte, Bd. IV, 2011, § 91 Rn. 32; *Tanneberger,* Die Sicherheitsverfassung, 2014, 144 f.; *Wolter*, GA 1988, 129, 141.

574 Zur Frage, wann ein Persönlichkeitsprofil vorliegt *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, 2023, 170 ff.

für ein Persönlichkeitsprofil werden können.[575] Eine Rundumüberwachung wäre absolut unzulässig, die Erkenntnisse unverwertbar; daher ist eine solche Überwachungsmaßnahme nicht vorschnell zu bejahen.[576] Bei der in dieser Arbeit vorrangig untersuchten Einsatzvariante automatisierter Gesichtserkennung – der Identitätsermittlung – ist nicht von einer besonderen Gefahr der Rundumüberwachung auszugehen. Denn bei dieser Ermittlungsmaßnahme wird nur mit Blick auf ein einzelnes Foto (höchstens einige wenige Fotos) die Identität eines Beschuldigten ermittelt.[577]

Die Gefahr einer Rundumüberwachung besteht dagegen grundsätzlich bei einer Verwendung automatisierter Gesichtserkennung zur *digitalen Beobachtung*, bei der Videoaufnahmen von verschiedenen Orten zusammengeführt werden, um weitere Informationen über den Verdächtigen zu erlangen.[578] Wird eine große Menge an Datenmaterial über eine Person per automatisierter Gesichtserkennung kombiniert, kann sich wie ein Mosaik[579] ein sehr detailliertes Bild des Betroffenen zusammensetzen.[580] Bei einer zu umfassenden Überwachung könnte die Menschenwürde verletzt werden. Daher wäre es bei dieser Einsatzvariante womöglich sinnvoll, das Verbot der Erstellung von Persönlichkeitsprofilen auch einfachgesetzlich ausdrücklich zu verbieten. (In diese Richtung gehen etwa § 14a Abs. 2 S. 5 HSOG, Art. 39 Abs. 3 S. 2 BayPAG, die mit Blick auf die automatisierte

575 BVerfGE 156, 63 (123) mwN; *Rudolf*, in: Merten/Papier, Handbuch der Grundrechte, Bd. IV, 2011, § 90 Rn. 67.

576 Huber/Voßkuhle/*Eichberger*, 8. Aufl. 2024, GG Art. 2 Rn. 315.

577 Dies bekräftigt auch erneut das oben herausgearbeitete Erfordernis, in der Ermächtigungsgrundlage für den Einsatz automatisierter Gesichtserkennung den *Zweck* der Maßnahme (Identifizierung unbekannter Verdächtiger) festzulegen; vgl. Kapitel II. A. I. 3. b). Denn dadurch wird sichergestellt, dass automatisierte Gesichtserkennung nicht ohne Weiteres für andere Zwecke genutzt wird, etwa, um weitere Informationen über den Verdächtigen zu erlangen – wodurch sich bei ausufernder Anwendung die Frage der Rundumüberwachung einer Person stellen würde.

578 Siehe zu dieser Einsatzvariante Kapitel I. C. II. 3.

579 Vgl. zur „mosaic theory" im US-amerikanischen Verfassungsrecht *Kerr*, Michigan Law Review 2012, 311; siehe auch *Wittmann*, ZaöRV 2013, 373, 392 ff.

580 Zu erhöhten Risiken für die Privatheit durch Kombination öffentlich verfügbarer Daten zu einem umfassenden Bericht *Solove*, Minnesota Law Review 2002, 1137, 1139 f. Speziell im Zusammenhang mit Gesichtserkennung *Ferguson*, Minnesota Law Review 2021, 1105, 1135; *Schindler*, Biometrische Videoüberwachung, 2021, 333 f.; vgl. in diese Richtung auch *Desoi*, Intelligente Videoüberwachung, 2018, 73; *Stettner*, Sicherheit am Bahnhof, 2017, 150.

Kennzeichenkontrolle grundsätzlich die Erstellung von Bewegungsbildern verbieten.)[581]

Interessanter für das in dieser Arbeit vorrangig untersuchte Einsatzszenario der Identitätsermittlung mit automatisierter Gesichtserkennung ist die Frage, inwieweit sich aus der Menschenwürde Grenzen für die Automatisierung dieses Prozesses ergeben. *Golla* leitet aus der Menschenwürde ein Recht ab, „nicht ungeprüft automatisierten Entscheidungen von einer gewissen Tragweite unterworfen zu werden";[582] dies solle jedoch nur bei einer „erheblichen Beeinträchtigung" gelten.[583] Er folgert dies daraus, dass die Menschenwürde garantiere, dass der Mensch nie „zum rechtlosen Objekt eines Verfahrens herabgewürdigt werden" darf. Diese Überlegungen erscheinen im Ansatz plausibel, bedürfen aber in Zukunft noch einer Konkretisierung und lassen viele Fragen offen.[584] Warum bedeutet es eine Herabwürdigung eines Menschen zum rechtlosen Objekt eines Verfahrens, wenn eine rein automatisierte Entscheidung einer gewissen Tragweite über

581 Vgl. zur Vermeidung einer „Rundumüberwachung" auch § 463a Abs. 4 StPO i. V. m. § 68a Abs. 1 S. 1 Nr. 12 StGB; hierzu etwa BeckOK StPO/*Coen*, 49. Ed., Stand: 1.10.2023, StPO § 463a Rn. 7 und *Schwabenbauer*, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, Kapitel G. Informationsverarbeitung im Polizei- und Strafverfahrensrecht, Rn. 171 Fn. 565. Verfassungsrechtlich zwingend ist eine ausdrückliche Regelung des Verbots der Rundumüberwachung allerdings nicht; das Bundesverfassungsgericht hält insoweit „allgemeine verfahrensrechtliche Sicherungen" für ausreichend, siehe BVerfGE 112, 304 (319 f.).

582 *Golla*, in: Chibanguza/Kuß/Steege, Künstliche Intelligenz, 2022, 2. Teil: § 9 A. KI-Einsatz bei der Polizei Rn. 12; *Golla*, DÖV 2019, 673, 676; *Golla*, in: Donath/Bretthauer u. a., Verfassungen – ihre Rolle im Wandel der Zeit. 59. Assistententagung Öffentliches Recht, 2019, 183, 189 f.

583 Verbreitet wird auch das grundsätzliche Verbot vollautomatisierter Entscheidungen nach Art. 22 Abs. 1 DSGVO (vgl. auch Art. 11 Abs. 1 JI-RL) als Ausdruck der Menschenwürde gesehen. Vgl. zu einer Nähe des grundsätzlichen Verbots vollautomatisierter Entscheidungen zur Menschenwürde etwa *Paal/Hüger*, MMR 2024, 540; *Radtke*, RDi 2024, 353, 355 f.; *Malorny*, RdA 2022, 170, 176; *Malorny*, JuS 2022, 289, 295; *Golla*, NJW 2021, 667, 672; *Golla*, in: Chibanguza/Kuß/Steege, Künstliche Intelligenz, 2022, 2. Teil: § 9 A. KI-Einsatz bei der Polizei Rn. 12 f.; Paal/Pauly/*Martini*, 3. Aufl. 2021, DSGVO Art. 22 Rn. 29b; *Geminn*, DÖV 2020, 172, 176; *Golla*, DÖV 2019, 673, 678 f.; *Golla*, in: Donath/Bretthauer u. a., Verfassungen – ihre Rolle im Wandel der Zeit. 59. Assistententagung Öffentliches Recht, 2019, 183, 196; *Orwat*, Diskriminierungsrisiken durch Verwendung von Algorithmen, 2019, 91 f.; *Ernst*, JZ 2017, 1026, 1030; *Martini*, DÖV 2017, 443, 452; in eine ähnliche Richtung auch *Vasel/Heck*, NVwZ 2024, 540, 544.

584 Vgl. außerdem zu der Frage, inwiefern die Menschenwürde als normativer Anknüpfungspunkt für Transparenzanforderungen an Algorithmen dienen kann *Sommerer*, Personenbezogenes Predictive Policing, 2020, 234 ff.

ihn getroffen wird? Warum liegt keine solche Objektivierung vor, wenn ein Mensch exakt dieselbe Entscheidung trifft? Um ein „Verfahren" handelt es sich in beiden Fällen. Auch wird in Zukunft weiter zu klären sein, wann eine Entscheidung überhaupt vollautomatisiert bzw. ungeprüft automatisiert abläuft. Wenn kein Mensch auch nur die theoretische Möglichkeit hat einzugreifen? Was, wenn Menschen beteiligt sind, aber aufgrund fehlenden Know-hows oder mangelnder Eingriffskompetenz faktisch nicht eingreifen? Was, wenn die beteiligten Menschen zwar das Know-how und die Eingriffskompetenz haben, aber (Stichwort: Automation bias) das Geschehen typischerweise nur abnicken? Jedenfalls dürfte Konsens bestehen, dass dystopische Szenarien wie eine strafrechtliche Verurteilung allein aufgrund eines rein automatisierten Verfahrens ohne jegliche menschliche Beteiligung der Menschenwürde widersprechen.[585] Auch lässt sich darüber nachdenken, ob die Menschenwürde es verbietet, allein aufgrund eines automatisierten Verfahrens (z. B. Treffer eines Gesichtserkennungssystems) eingriffsintensive Ermittlungsmaßnahmen ohne jegliche menschliche Überprüfung zu veranlassen. Ein solches Szenario steht allerdings nicht im Raum, da die Strafverfolgungsbehörden auf absehbare Zeit jedenfalls – wenn auch nicht geschulte Gesichtserkennungsprüfer – weiterhin einen menschlichen Polizisten die Treffer überprüfen lassen werden. Das gilt schon deshalb, weil die Durchführung von Ermittlungsmaßnahmen ohnehin regelmäßig ein menschliches Handeln (z. B. Hausdurchsuchung, Befragung) erfordert.

III. Fazit zu den verfassungsrechtlichen Anforderungen an eine Rechtsgrundlage

Die Erstellung der Embeddings für die Gesichtserkennung, der Abgleich und die „Treffer" (Auftauchen auf der Kandidatenliste) begründen jeweils eigenständige Eingriffe in das Recht auf informationelle Selbstbestimmung. Jedenfalls der Abgleich und die „Treffer" sind erhebliche Eingriffe. Eine Ermächtigung, die den Einsatz automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger erlaubt, muss verhältnismäßig sein. Die Aufklärung von Straftaten ist in dieser Hinsicht ein legitimer Zweck und muss nicht auf besonders schwere Straftaten beschränkt werden. Angesichts der Heimlichkeit der Maßnahme und der besonderen Fehleranfälligkeit

585 Vgl. auch allgemein zur Automatisierung der Rechtsprechung *Bernzen*, RDi 2023, 132, 136; siehe auch *Nink*, Justiz und Algorithmen, 2021, 348 ff.

erscheinen Benachrichtigungspflichten verfassungsrechtlich geboten. Eine aufsichtliche Kontrolle der Maßnahmen ist vorzusehen und vom Gesetzgeber näher auszugestalten. Sinnvoll, aber verfassungsrechtlich nicht näher konkretisiert sind Beobachtungs- und Evaluationspflichten des Gesetzgebers und Berichtspflichten der Strafverfolgungsbehörden gegenüber Parlament und Öffentlichkeit. Wird Videomaterial ausgewertet, das im Rahmen einer Versammlung gefertigt wurde, so ist bei der Auslegung der Ermächtigungsgrundlage für die Gesichtserkennung die besondere Bedeutung der Versammlungsfreiheit zu berücksichtigen. Eine mittelbare Diskriminierung als Verstoß gegen Art. 3 Abs. 3 GG kommt in Betracht, wenn Gesichtserkennungssysteme verwendet werden, die große Unterschiede in der Erkennungsleistung für verschiedene Bevölkerungsgruppen aufweisen und daher deutlich häufiger Ermittlungsmaßnahmen gegen Unschuldige durchgeführt werden, die einer von Art. 3 Abs. 3 GG geschützten Gruppe angehören.

B. Europäisches Recht

Weiterhin ist zu untersuchen, welche zusätzlichen Anforderungen das europäische Recht an den Einsatz automatisierter Gesichtserkennung zur Ermittlung der Identität unbekannter Verdächtiger stellt. Dabei sind das Unionsrecht und die Europäische Menschenrechtskonvention näher in den Blick zu nehmen.

I. Unionsrecht

Auf EU-Ebene macht die KI-Verordnung nähere Vorgaben zum Einsatz automatisierter Gesichtserkennung in der Strafverfolgung. Zudem ist zu untersuchen, ob die JI-Richtlinie und die EU-Grundrechte-Charta konkrete Anforderungen stellen.

1. KI-Verordnung

Die EU hat sich zum Ziel gesetzt, das weltweit erste umfangreiche Gesetz zur Regulierung Künstlicher Intelligenz zu erlassen.[586] Nach zahlreichen

586 Instruktiv zur Einordnung etwa *Nemitz*, MMR 2024, 603.

Debatten und zähem Ringen einigten sich Kommission, Rat und Parlament. Am 1. August 2024 trat die KI-VO in Kraft.[587] Die Vorschriften der KI-Verordnung zu biometrischer Fernidentifizierung – dazu gehört automatisierte Gesichtserkennung – enthalten keine Ermächtigung zum Einsatz biometrischer Fernidentifizierung.[588] Sie setzen eine nationale Regelung voraus und stellen zusätzliche Anforderungen.

In den folgenden Abschnitten wird herausgearbeitet, welche Mindestanforderungen die KI-Verordnung an den Einsatz automatisierter Gesichtserkennung in der Strafverfolgung stellt, insbesondere mit Blick auf das in dieser Arbeit vorrangig betrachtete Szenario der Identifizierung unbekannter Verdächtiger.[589] Es wird zunächst erläutert, dass nachträgliche Gesichtserkennung in der KI-Verordnung als Hochrisiko-KI eingestuft wird. Danach werden die allgemeinen Vorgaben für Hochrisiko-KI-Systeme vorgestellt und zuletzt wird auf die spezifischen Vorschriften für den Einsatz nachträglicher Gesichtserkennung in der Strafverfolgung eingegangen.

a) Nachträgliche Gesichtserkennung als Hochrisiko-KI

Die KI-Verordnung der EU verfolgt einen risikobasierten Ansatz. Anstatt für einzelne Sektoren spezifische Vorgaben zu erlassen, werden KI-Anwendungen bereichsübergreifend mit Blick auf ihre Risikoeinstufung reguliert.[590] KI-Anwendungen, die als unannehmbar risikoreich kategorisiert werden, sind grundsätzlich verboten (Art. 5 KI-VO).[591] Anwendungen mit hohem Risiko sind streng reguliert und können nur dann auf den EU-Markt gebracht oder in Betrieb genommen werden, wenn sie strenge Anforderungen erfüllen und eine Ex-ante-Konformitätsbewertung durchlaufen.[592] Bei Anwendungen mit geringem Risiko müssen die in Art. 50 KI-VO geregelten Transparenzanforderungen gewahrt werden. Für KI-Anwendun-

587 Zum Geltungsbeginn der einzelnen Vorgaben siehe Art. 113 KI-VO.

588 So auch *Chibanguza/Steege*, NJW 2024, 1769, 1772.

589 Siehe zur Regulierung biometrischer Fernidentifizierungssysteme in der Strafverfolgung im KI-Verordnungsentwurf der EU-Kommission *Hahn*, ZfDR 2023, 142; für eine Gegenüberstellung der Entwürfe des EU-Parlaments und der EU-Kommission siehe *Feuerstack/Becker/Hertz*, ZfDR 2023, 421.

590 Die folgenden Abschnitte beruhen teilweise auf *Hahn*, ZfDR 2023, 142. Zum risikobasierten Ansatz der KI-Verordnung siehe näher *Roth-Isigkeit*, MMR 2024, 621.

591 Zu diesen auch *Rostalski/Weiss*, in: Hilgendorf/Roth-Isigkeit, Die neue Verordnung der EU zur Künstlichen Intelligenz, 2023, 35 (noch zum Verordnungsentwurf).

592 Siehe insbesondere Art. 8 ff. KI-VO.

gen mit minimalem Risiko sieht die KI-Verordnung keine Anforderungen vor, sie müssen aber andere EU-Vorgaben, insbesondere die DSGVO, einhalten; freiwillig können Verhaltenskodizes befolgt werden (vgl. Art. 95 KI-VO).

Die KI-Verordnung enthält auch Vorschriften für „biometrische Fernidentifizierungssysteme", die zur Strafverfolgung eingesetzt werden.[593] Die Verwendung von Echtzeit-Fernidentifizierung in öffentlich zugänglichen Räumen zur Strafverfolgung[594] wird als unannehmbares Risiko eingestuft und grundsätzlich verboten (Art. 5 Abs. 1 lit. h KI-VO).[595] Biometrische Fernidentifizierungssysteme zur *nachträglichen* Auswertung werden dagegen als Hochrisiko-KI-Anwendungen eingeordnet und nicht verboten, siehe Art. 6 Abs. 2 KI-VO i. V. m. Anhang III Nr. 1 lit. a.[596]

aa) Gesichtserkennung als Fernidentifizierung

Unter einem biometrischen Fernidentifizierungssystem versteht die KI-Verordnung „ein KI-System, das dem Zweck dient, natürliche Personen ohne ihre aktive Einbeziehung und in der Regel aus der Ferne durch Abgleich der biometrischen Daten einer Person mit den in einer Referenzdatenbank gespeicherten biometrischen Daten zu identifizieren" (Art. 3 Nr. 41

593 Allerdings ist die Regelungskompetenz der EU mit Blick auf den Einsatz biometrischer Fernidentifizierung in der Strafverfolgung äußerst zweifelhaft, hierzu näher *Schindler/Schomberg,* in: Friedewald/Roßnagel/Heesen/Krämer/Lamla, Künstliche Intelligenz, Demokratie und Privatheit, 2022, 103, 123 ff.; kritisch auch *Pilniok,* DÖV 2024, 581, 583; *Linardatos*, GPR 2022, 58, 59; *Martini,* NVwZ-Extra 1-2/2022, 1, 16; *Valta/Vasel*, ZRP 2021, 142, 143.

594 Die deutsche Übersetzung der KI-Verordnung spricht hier von einem Einsatz „zu Strafverfolgungszwecken", die verbindliche englische Fassung hingegen von „for the purposes of law enforcement", worunter nicht nur die Strafverfolgung, sondern insbesondere auch die Gefahrenabwehr fällt.

595 Diese Vorschriften sollen als leges speciales zu Art. 10 JI-RL gelten, der Vorgaben enthält für die Verarbeitung biometrischer Daten im Zusammenhang mit Strafverfolgung oder Gefahrenabwehr, vgl. ErwG 38 KI-VO.

596 Echtzeit-Fernidentifizierung wird, sofern sie in einem Mitgliedsstaat zugelassen wird, ebenfalls als Hochrisiko-KI eingeordnet, siehe Anhang III Nr. 1 lit. a KI-VO und ErwG 54.

KI-VO).[597] (Nicht darunter fallen KI-Systeme[598], die für die biometrische Verifizierung verwendet werden sollen, deren einziger Zweck also darin besteht, zu bestätigen, dass eine bestimmte natürliche Person die Person ist, für die sie sich ausgibt.)[599]

Bei den in Embeddings repräsentierten Gesichtsmerkmalen[600] handelt es sich ohne Weiteres um biometrische Daten. „Biometrische Daten" sind nach der KI-Verordnung „mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten" (Art. 3 Nr. 34 KI-VO).[601]

Bei der Verwendung welcher biometrischen Merkmale eine Identifizierung „aus der Ferne" („at a distance") erfolgt, ist nicht ganz klar.[602] Die KI-Verordnung scheint dabei an die physische Distanz zwischen dem biometrischen Merkmal und dem Sensor des Erkennungssystems anzuknüpfen.[603] Die Erkennung anhand von Gesicht oder Gang ist aus mehreren

---

597 Kritisch zur ursprünglichen Definition des biometrischen Fernidentifizierungssystems im KI-Verordnungsentwurf *Hahn*, ZfDR 2023, 142, 146.

598 Der Begriff des KI-Systems ist in Art. 3 Nr. 1 KI-VO definiert als „ein maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen können". Zur Kritik an diesem Begriff *Wendehorst/Nessler/Aufreiter/Aichinger*, MMR 2024, 605.

599 Dies wurde nun sinnvollerweise klargestellt und ergibt sich aus Anhang III Nr. 1 lit. a i. V. m. Art. 3 Nr. 36 KI-VO und ErwG 15, 17, 54; Forderung nach einer solchen Klarstellung auch bereits bei *Hahn*, ZfDR 2023, 142, 146.

600 Zum technologischen Hintergrund Kapitel I. E. III.

601 Dieselbe Definition findet sich bereits in Art. 3 Nr. 13 JI-RL und Art. 4 Nr. 14 DSGVO.

602 *Hahn*, ZfDR 2023, 142, 153 f.

603 Hingegen hatten etwa – noch im Hinblick auf den KI-Verordnungsentwurf der EU-Kommission – *Schindler*, ZD-Aktuell 2021, 05221 und *Schindler/Schomberg*, in: Friedewald/Roßnagel/Heesen/Krämer/Lamla, Künstliche Intelligenz, Demokratie und Privatheit, 2022, 103, 115) dafür plädiert, statt (allein) auf die physische Distanz zwischen biometrischem System und Betroffenem für den Begriff der „Fernidentifizierung" auch darauf abstellen, ob die Erkennung ohne Mitwirkung und damit meist ohne Wissen der Person möglich ist. Andere grenzten Systeme zur Fernidentifizierung von solchen der „Nahidentifizierung" ab, bei denen sich die Person bewusst in einem kontrollierten Bereich begeben, siehe *Orssich*, EuZW 2022, 254 Fn. 31. Die in der finalen Fassung der KI-Verordnung nun gewählte Formulierung „ohne ihre aktive Einbeziehung *und* in der Regel aus der Ferne" (Hervorhebung

Metern Entfernung möglich, Gesichtserkennung ist daher ohne Weiteres eine Identifizierung aus der Ferne.[604] Nicht erfasst sind andererseits wohl jedenfalls (trotz der Formulierung „in der Regel") berührungsbasierte Systeme zur Fingerabdruckerkennung[605] oder Retina-Scans[606].

Wann der Abgleich biometrischer Daten einer Person „ohne ihre aktive Einbeziehung" („without their active involvement") erfolgt, ist ebenfalls nicht ganz eindeutig. Umgekehrt gefragt: Wann ist ein Betroffener aktiv einbezogen in den Abgleich biometrischer Daten? Wenn er Kenntnis von der Maßnahme hat? Wenn er ihr zustimmt? Aktiv mitwirkt? Relevant wird diese Frage etwa in folgender Situation: Bei der Passkontrolle mittels Gesichtserkennung am Flughafen begibt sich die Person bewusst und aktiv in den Kontrollbereich und wirkt daran mit, dass der Abgleich ihrer biometrischen Daten stattfinden kann. Wird nur ein Abgleich mit ihren eigenen biometrischen Daten aus dem Reisepass vorgenommen, handelt es sich um eine Verifizierung, keine Identifizierung (also auch nicht um eine biometrische Fernidentifizierung). Was aber, wenn die Person mit einer Liste gesuchter Straftäter oder Terrorverdächtiger abgeglichen wird? War sie dann aktiv einbezogen in den Datenabgleich, weil sie sich bewusst in den Kontrollbereich begeben hat? Oder nicht, weil sie nicht wusste, dass ihre biometrischen Daten (auch) mit denen anderer Personen abgeglichen werden, also zur Identifizierung verwendet werden? Wenn man hier – nicht gänzlich unplausibel – eine aktive Einbeziehung bejaht, käme man mit der Definition des Art. 3 Nr. 41 KI-VO zu dem Ergebnis, dass es sich *nicht* um biometrische Fernidentifizierung handelt; es würden dann also nicht

---

J. H.) nimmt die fehlende Involvierung der Betroffenen nun als eigenes Merkmal auf („ohne ihre aktive Einbeziehung"). Das spricht dafür, dass mit „aus der Ferne" tatsächlich an die physische Distanz angeknüpft wird.

604 Dies dürfte schon allein deshalb gelten, weil die gesamte politische und mediale Diskussion über die Regulierung biometrischer Fernidentifizierung in der KI-Verordnung fast ausschließlich mit Blick auf Gesichtserkennung geführt wurde.

605 So auch *Schindler/Schomberg*, in: Friedewald/Roßnagel/Heesen/Krämer/Lamla, Künstliche Intelligenz, Demokratie und Privatheit, 2022, 103, 115. Denn hier besteht kein Abstand zwischen Finger und dem System.

606 Die Retina (Netzhaut) befindet sich am hinteren Teil des Auges und kann nur aus der Entfernung weniger Zentimeter gescannt werden, vgl. *Uhl*, in: Uhl/Busch/Marcel/Veldhuis, Handbook of Vascular Biometrics, 2020, 3, 8 f.; *Semerád/Drahanský*, in: Uhl/Busch/Marcel/Veldhuis, Handbook of Vascular Biometrics, 2020, 309, 313; die Person muss zudem ihren Kopf für etwa 10–30 Sekunden stillhalten. Siehe hierzu bereits *Hahn*, ZfDR 2023, 142, 153, auch mit Erläuterungen, warum für Iriserkennung noch weniger eindeutig ist, ob von einer Erkennung „aus der Ferne" ausgegangen werden kann.

einmal die erhöhten Anforderungen für Hochrisiko-Systeme nach Art. 8 ff. KI-VO zu Dokumentation, menschlicher Kontrolle usw. gelten.[607]

Grundsätzlich wird man aber davon ausgehen können, dass die meisten Anwendungen automatisierter Gesichtserkennung in der Strafverfolgung unter den Begriff des biometrischen Fernidentifizierungssystems des Art. 3 Nr. 41 KI-VO fallen.

bb) Einsatz zur Identifizierung unbekannter Verdächtiger

Insbesondere ist das in dieser Arbeit vorrangig untersuchte Einsatzszenario der Identifizierung unbekannter Verdächtiger „biometrische Fernidentifizierung" im Sinne der KI-Verordnung.

Die KI-Verordnung unterscheidet nicht zwischen verschiedenen Einsatzszenarien biometrischer Fernidentifizierung in der Strafverfolgung wie etwa Echtzeit-Fahndung, Identifizierung unbekannter Verdächtiger in erkennungsdienstlichen Datenbanken, Auswertung umfangreichen Datenmaterials per Gesichtserkennung, digitale Beobachtung usw.[608] Stattdessen differenziert die KI-Verordnung nur zwischen Echtzeit-Fernidentifizierung in öffentlich zugänglichen Räumen zum Zwecke der Strafverfolgung einerseits und allen anderen Anwendungsfällen andererseits.[609] Zu letzteren gehört daher auch die nachträgliche biometrische Fernidentifizierung in der Strafverfolgung. Es ist davon auszugehen, dass damit auch der Einsatz automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger erfasst werden soll.

In dem ursprünglichen Entwurf einer KI-Verordnung der EU-Kommission ging dies noch nicht eindeutig aus dem Wortlaut der Definition hervor. Art. 3 Nr. 36 KI-VO-E definierte ein biometrisches Fernidentifizierungssystem als „ein KI-System, das dem Zweck dient, natürliche Personen aus der Ferne durch Abgleich der biometrischen Daten einer Person mit den in einer Referenzdatenbank gespeicherten biometrischen Daten zu identifizieren, ohne dass der Nutzer des KI-Systems vorher weiß, ob die Person an-

607 Vgl. auch bereits *Hahn*, ZfDR 2023, 142, 154.

608 Zu verschiedenen Szenarien Kapitel I. C. II.

609 Hierzu kritisch *Hahn*, ZfDR 2023, 142, 162 f. Zu diesen anderen Anwendungsfällen zählt etwa der Einsatz von Echtzeit-Fernidentifizierung durch Private, der Einsatz von Echtzeit-Fernidentifizierung zur Strafverfolgung in *nicht* öffentlich zugänglichen Räumen oder online sowie der nachträgliche Einsatz biometrischer Fernidentifizierung durch Strafverfolgung und Private.

wesend sein wird und identifiziert werden kann". Bei genauer Betrachtung passte das Anwendungsszenario der Identifizierung unbekannter Verdächtiger allerdings nicht zu der Definition in Art. 3 Nr. 36 KI-VO-E. Problematisch war hierbei der Passus „ohne dass der Nutzer des KI-Systems vorher weiß, ob die Person *anwesend* sein wird und identifiziert werden kann" (Hervorhebung J. H.).[610] Damit erfasste der Entwurf insbesondere den Einsatz biometrischer Fernidentifizierung zur Echtzeit-Fahndung. Denn wird etwa das Videomaterial eines Flughafens in Echtzeit gescannt, um herauszufinden, ob sich ein gesuchter Straftäter dort aufhält, dann weiß der Nutzer des KI-Systems nicht, ob dieser „anwesend" ist. Gemeint dürfte damit gewesen sein, dass unklar ist, ob die gesuchte Person an dem Ort anwesend ist, von dem Aufnahmen angefertigt werden/wurden, die nun durchsucht werden.[611] Das Einsatzszenario der Identifizierung unbekannter Verdächtiger in einer staatlichen Lichtbilddatenbank wurde damit aber sprachlich gar nicht erfasst. Der Passus „ohne dass der Nutzer[612] des KI-Systems vorher weiß, ob die Person *anwesend* sein wird und identifiziert werden kann" (Hervorhebung J. H.) passte hier nicht. Wenn beispielsweise ein Polizist (der KI-Nutzer) einen bei einem Ladendiebstahl gefilmten Täter (die Person) identifizieren will, dann weiß er, dass diese Person sich auf dem Bildmaterial befindet, aber nicht, ob diese Person *in der Datenbank vorhanden* ist. Die Definition des Art. 3 Nr. 36 KI-VO-E umfasste daher die Verwendung biometrischer Erkennung zur Identitätsermittlung gar nicht. Der Einsatz automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger wäre damit von der KI-Verordnung gar nicht geregelt worden. Dies konnte kaum gewollt gewesen sein, denn dabei handelt es sich um das in den EU-Staaten mit Abstand am weitesten verbreitete[613] Einsatzszenario biometrischer Fernidentifizierung. Daher war davon auszugehen, dass die Verwendung automatisierter Gesichtserkennung zur Ermittlung der Identität unbekannter Verdächtiger eine (nachträgliche) Fernidentifizierung im Sinne des Art. 3 Nr. 36 KI-VO-E war, auch wenn die Definition diese Einsatzvariante eigentlich nicht erfasste.[614]

610 Zum Ganzen auch bereits *Hahn*, ZfDR 2023, 142, 151 f.
611 *Hahn*, ZfDR 2023, 142, 151.
612 Der finale Text der KI-Verordnung verwendet nicht mehr den Begriff des „Nutzers", sondern nunmehr den des „Betreibers".
613 Zu den hierfür in den verschiedenen EU-Staaten verwendeten Datenbanken siehe Summary report of the project „Towards the European Level Exchange of Facial Images" (TELEFI) 2021, 11 f., https://perma.cc/T6NE-GTRV.
614 *Hahn*, ZfDR 2023, 142, 151.

Mit der nun überarbeiteten Definition des „biometrischen Fernidentifizierungssystems" in der finalen Fassung der KI-Verordnung in Art. 3 Nr. 41 KI-VO besteht diese Unklarheit nicht mehr. Ein „KI-System, das dem Zweck dient, natürliche Personen ohne ihre aktive Einbeziehung und in der Regel aus der Ferne durch Abgleich der biometrischen Daten einer Person mit den in einer Referenzdatenbank gespeicherten biometrischen Daten zu identifizieren"; dies trifft auf ein Gesichtserkennungssystem zu, das zur Identifizierung unbekannter Verdächtiger verwendet wird. Insbesondere findet der Abgleich ohne aktive Einbeziehung der betroffenen Personen (unbekannter Verdächtiger und Personen in den Datenbanken) statt, ungeachtet dessen, ob damit Kenntnis, Zustimmung oder aktive Mitwirkung gemeint ist.[615] Dass diese Einsatzvariante von Gesichtserkennung erfasst sein soll, zeigt sich auch daran, dass Art. 26 Abs. 10 KI-VO diese in einem Satz erwähnt („zur erstmaligen Identifizierung eines potenziellen Verdächtigen auf der Grundlage objektiver und nachprüfbarer Tatsachen, die in unmittelbarem Zusammenhang mit der Straftat stehen"). Der Einsatz automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger ist daher biometrische Fernidentifizierung im Sinne der KI-Verordnung.

b) Vorgaben für Hochrisiko-KI-Systeme

Nach Art. 6 Abs. 2 KI-VO i. V. m. Anhang III Nr. 1 gelten unter anderem KI-Systeme, die bestimmungsgemäß für die nachträgliche biometrische Fernidentifizierung natürlicher Personen verwendet werden sollen, als Hochrisiko-KI-Systeme. Da die Verwendung automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger (wie oben gezeigt) hierunter fällt, gelten für die hierfür eingesetzten Systeme die in den folgenden Abschnitten dargelegten Vorgaben für Hochrisiko-KI-Systeme. Gesichtserkennungssysteme müssen daher die Vorgaben erfüllen, die für alle Hochrisiko-KI-Systeme Anwendung finden.[616]

615 Da es auf den *Abgleich* ankommt, ist auch nicht entscheidend, ob die Personen in die Erstellung der abzugleichenden Fotos aktiv einbezogen waren.

616 Insbesondere sind gem. Art. 8 Abs. 1 KI-VO die Vorgaben der Art. 9 bis 15 KI-VO einzuhalten; zu diesen näher *Braun Binder/Egli*, MMR 2024, 626. Diese Anforderungen gehen zurück auf Empfehlungen der von der EU-Kommission eingesetzten unabhängigen High Level Expert Group on Artificial Intelligence, siehe *High Level Expert Group on Artificial Intelligence*, The Assessment List for Trustworthy Artificial Intelligence for self assessment (ALTAI), 17.7.2020.

Diese muss in erster Linie der Anbieter erfüllen.[617] Anbieter ist gem. Art. 3 Nr. 3 KI-VO „eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System oder ein KI-Modell mit allgemeinem Verwendungszweck entwickelt oder entwickeln lässt und es unter ihrem eigenen Namen oder ihrer Handelsmarke in Verkehr bringt oder das KI-System unter ihrem eigenen Namen oder ihrer Handelsmarke in Betrieb nimmt, sei es entgeltlich oder unentgeltlich". Im Falle des Einsatzes automatisierter Gesichtserkennungssysteme kommt hier sowohl das Unternehmen in Betracht, welches das System hergestellt hat, als auch die Strafverfolgungsbehörde, die das System entwickeln lässt (seltener: selbst entwickelt).[618]

aa) Konformitätsbewertungsverfahren

Nach Art. 43 KI-VO müssen Hochrisiko-KI-Systeme vor dem Inverkehrbringen oder der Inbetriebnahme ein Konformitätsbewertungsverfahren durchlaufen,[619] um die Konformität mit technischen Standards sicherzustellen.[620] Dies dient dazu, bereits vor dem Einsatz des Systems mögliche Fehler zu erkennen und zu beheben, bevor eine Gefahr für die Betroffenen eintreten kann.[621] Auch soll damit ein hohes Maß an Vertrauenswürdigkeit gewährleistet werden.[622] Im Falle biometrischer Fernidentifizierungssyste-

617 Art. 16 lit. a KI-VO. Allerdings treffen diese Pflichten gem. Art. 25 KI-VO unter Umständen auch andere an der Wertschöpfungskette von KI-Systemen Beteiligte. Vor dem Inverkehrbringen oder der Inbetriebnahme eines Systems zur automatisierten Gesichtserkennung hat der Anbieter (oder gegebenenfalls sein Bevollmächtigter) gem. Art. 49 Abs. 1 KI-VO zudem sich und sein System in der in Art. 71 KI-VO genannten EU-Datenbank zu registrieren.

618 Dass gerade auch die Strafverfolgungsbehörden selbst Anbieter im Sinne des Art. 3 Nr. 3 KI-VO sein können, zeigt implizit auch Art. 78 Abs. 3 KI-VO („Handeln Strafverfolgungs-, […]behörden als Anbieter von in Anhang III Nummer 1, 6 oder 7 genannten Hochrisiko-KI-Systemen […]").

619 Diese Pflicht trifft gem. Art. 16 lit. f KI-VO den Anbieter.

620 Näher zum Konformitätsbewertungsverfahren (noch zum Verordnungsentwurf der EU-Kommission) *Spindler*, CR 2021, 361, 366 u. 369 ff. und *Ebert/Spiecker gen. Döhmann*, NVwZ 2021, 1188, 1191; siehe auch *Hoffmann*, Der nichtstaatliche Einsatz biometrischer Gesichtserkennungssysteme nach der DSGVO, 2023, 280 f.; *Bomhard/Merkle*, RDi 2021, 276, 281.

621 *Hoffmann*, Der nichtstaatliche Einsatz biometrischer Gesichtserkennungssysteme nach der DSGVO, 2023, 281; *Hoffmann*, K&R 2021, 369, 371.

622 ErwG 123.

me ist gem. Art. 43 Abs. 1 KI-VO grundsätzlich eine externe Konformitätsbewertung erforderlich. Eine interne Konformitätsbewertung ist nur dann zulässig, wenn mit Blick auf alle gesetzlichen Anforderungen einschlägige harmonisierte Normen existieren und wenn der Anbieter diese bei der Prüfung des KI-Systems vollumfänglich anwendet.[623]

Bei einer wesentlichen Änderung muss das Hochrisiko-KI-System nach Art. 43 Abs. 4 S. 1 KI-VO einem erneuten Konformitätsbewertungsverfahren unterzogen werden. Dabei ist nicht ganz klar, wann eine Änderung „wesentlich" („substantial") ist.[624] Für Systeme zur biometrischen Fernidentifizierung, also auch Gesichtserkennungssysteme, dürfte dies typischerweise nicht bereits dann der Fall sein, wenn neue Berechnungsmethoden für die Embeddings verwendet werden (z. B. andere künstliche neuronale Netze zur Extraktion der Embeddings).[625] Laut ErwG 128 liegt eine wesentliche Änderung beispielsweise bei einer Änderung des Betriebssystems oder der Softwarearchitektur vor; die Verwendung einer anderen Berechnungsmethode (die beispielsweise eine andere Gewichtung der Features zugrunde legt) verändert aber nicht die Softwarearchitektur des Gesichtserkennungssystems.

Das Risiko eines Gesichtserkennungssystems würde sich allerdings erheblich verändern, wenn im Bereich der Strafverfolgung weitere Datenbanken herangezogen würden; denn dann wären mehr Menschen von einer Beeinträchtigung ihrer informationellen Selbstbestimmung und möglichen

623 Nach Anhang VI kann der Betreiber die Konformität durch interne Kontrollen nachweisen, die sich auf das nach Art. 17 KI-VO zu etablierende Qualitätsmanagementsystem sowie die technische Dokumentation und die Produktbeobachtung beziehen; dann müssen aber harmonisierte technische Standards oder die „common specifications" der EU-Kommission zur Verfügung stehen, hierzu auch *Gerdemann*, MMR 2024, 614, 617; *Ebert/Spiecker gen. Döhmann*, NVwZ 2021, 1188, 1191; *Spindler*, CR 2021, 361, 370.

624 In Art. 3 Nr. 23 KI-VO wird eine „wesentliche Veränderung" definiert als „eine Veränderung eines KI-Systems nach dessen Inverkehrbringen oder Inbetriebnahme, die in der vom Anbieter durchgeführten ursprünglichen Konformitätsbewertung nicht vorgesehen oder geplant war und durch die die Konformität des KI-Systems mit den Anforderungen in Kapitel III Abschnitt 2 beeinträchtigt wird oder die zu einer Änderung der Zweckbestimmung führt, für die das KI-System bewertet wurde".

625 *Hoffmann*, Der nichtstaatliche Einsatz biometrischer Gesichtserkennungssysteme nach der DSGVO, 2023, 281, ist der Auffassung, dass es sich in einem solchen Fall um eine bereits vorab bestimmte Änderung handeln dürfte. Nach Art. 43 Abs. 4 S. 2 KI-VO gelten Änderungen des Hochrisiko-KI-Systems und seiner Leistung, die vom Anbieter zum Zeitpunkt der ursprünglichen Konformitätsbewertung vorab festgelegt wurden und in den Informationen der technischen Dokumentation gemäß Anhang IV Nr. 2 lit. f enthalten sind, nicht als wesentliche Veränderung.

Fehlern betroffen. Eine solche Veränderung dürfte jedoch keine wesentliche Veränderung des KI-Systems im Sinne des Art. 43 Abs. 4 S. 1 KI-VO darstellen, da die *technische* Funktionsweise unverändert bleibt.

bb) Risikomanagementsystem

Nach Art. 9 KI-VO ist ein Risikomanagementsystem einzurichten, um während des gesamten Lebenszyklus des KI-Systems tatsächliche und potenzielle[626] Risiken zu erkennen und geeignete Gegenmaßnahmen zu ergreifen.[627] Allerdings wird zu Recht darauf hingewiesen, dass der für das Risikomanagement verantwortliche Anbieter hier in einem Interessenskonflikt steht: Je risikoreicher er das KI-System einschätzt, desto strengere Gegenmaßnahmen muss er ergreifen.[628]

cc) Datenqualität

Art. 10 KI-VO enthält Kriterien für die Qualität der Trainings-, Validierungs- und Testdatensätze des KI-Systems. Die Vorgaben wurden gegenüber dem Verordnungsentwurf der EU-Kommission abgeschwächt, sie sind dadurch jedoch auch realistischer zu erfüllen. Insbesondere müssen die Daten „relevant, hinreichend repräsentativ und so weit wie möglich fehlerfrei und vollständig" (Art. 10 Abs. 3 KI-VO), während im Verordnungsentwurf der EU-Kommission noch die Rede davon war, dass die Daten „relevant, repräsentativ, fehlerfrei und vollständig" sein müssen. Angesichts der großen Anzahl benötigter Daten für ein KI-System wäre eine völlige Fehlerfreiheit aber unmöglich.[629] Die Daten sind außerdem nach Art. 10 Abs. 2 lit. f KI-VO zu untersuchen im Hinblick auf mögliche Verzerrungen

626 Art. 9 Abs. 2 lit. c KI-VO („Bewertung *anderer möglicherweise* auftretender Risiken"); so auch bereits Abänderung 265 der Abänderungen des EU-Parlaments zum KI-Verordnungsentwurf der EU-Kommission.

627 Art. 9 Abs. 2 lit. d KI-VO.

628 *Hoffmann*, Der nichtstaatliche Einsatz biometrischer Gesichtserkennungssysteme nach der DSGVO, 2023, 281 f.; *Hoffmann*, K&R 2021, 369, 372.

629 *Bomhard/Merkle*, RDi 2021, 276, 280; *Ebers/Hoch/Rosenkranz/Ruschemeier/Steinrötter*, RDi 2021, 528, 533; speziell zur Unmöglichkeit eines fehlerfreien Datensatzes im Kontext von Gesichtserkennung auch *Schindler/Schomberg*, in: Friedewald/Roßnagel/Heesen/Krämer/Lamla, Künstliche Intelligenz, Demokratie und Privatheit, 2022, 103, 121.

(Biases), die die Gesundheit und Sicherheit von Personen beeinträchtigen, sich negativ auf die Grundrechte auswirken oder zu einer nach den Rechtsvorschriften der Union verbotenen Diskriminierung führen könnten.[630]

Grundsätzlich sind diese Vorgaben sinnvoll, um die Leistungsfähigkeit von KI-Systemen sicherzustellen; die verwendeten Trainingsdaten sind hierfür ein entscheidender Faktor. Auch für Gesichtserkennungssysteme spielt die Qualität und Repräsentativität der Daten eine zentrale Rolle, damit eine vergleichbare Erkennungsgenauigkeit für verschiedene Bevölkerungsgruppen erreicht werden kann.[631] Diese Anforderungen an die Daten werden jedoch zu Recht kritisiert, da sie so allgemein formuliert schwierig umzusetzen,[632] *Hacker/Wessel* kritisieren zudem eine „mangelnde Koordination" mit den Vorschriften gegen Diskriminierung.[633]

Nicht adressiert werden durch die Vorgaben für die Datenqualität außerdem andere Gründe für Verzerrungen und daraus folgende Ungleichbehandlung,[634] die gerade beim Einsatz automatisierter Gesichtserkennung in der Strafverfolgung eine Rolle spielen. So entscheidet etwa die Frage, wer in einer zum Abgleich herangezogenen Datenbank gespeichert ist, darüber, wer überhaupt als – womöglich falscher – Treffer gefunden werden kann. Werden Personen einer bestimmten Bevölkerungsgruppe aufgrund von Verzerrungen der Polizisten häufiger kontrolliert, als verdächtig angesehen und erkennungsdienstlich behandelt, dann tauchen diese Personen häufiger in polizeilichen Datenbanken auf und sind damit auch dem Risiko ausgesetzt, fehlerhaft identifiziert zu werden.[635] Die KI-Verordnung nimmt solche möglichen „sozialen Verzerrungen" nicht in den Blick, sie adressiert in diesem Zusammenhang nur statistische Verzerrungen durch nicht-repräsentative Trainings-, Validierungs- und Testdatensätze.

630 Im Verordnungsentwurf der EU-Kommission war noch allgemein formuliert, dass die Daten generell im Hinblick auf mögliche Verzerrungen (Biases) untersucht werden müssen.

631 Kapitel I. E. IV. 2. a) und 5.

632 *Floridi*, Philosophy & Technology 2021, 215, 219; *Hoffmann*, K&R 2021, 369, 372; *Roos/Weitz*, MMR 2021, 844, 851; *Valta/Vasel*, ZRP 2021, 142, 144.

633 *Hacker/Wessel,* in: BMUV/Rostalski, Künstliche Intelligenz, 2022, 53, 62 f.

634 So auch mit anschaulichem Beispiel *Guijarro Santos*, ZfDR 2023, 23, 30 f., die zu Recht darauf hinweist, dass datenbasierte Diskriminierung aufgrund *sozialer* Datenbiases durch statistische Sorgfaltsstandards nicht verhindert werden können.

635 Vgl. bereits Kapitel I. E. IV. 5.

dd) Technische Dokumentation

Art. 11 KI-VO sieht vor, dass eine technische Dokumentation eines Hochrisiko-KI-Systems erstellt wird, bevor dieses System in Verkehr gebracht oder in Betrieb genommen wird. Diese Dokumentation ist stets auf dem neuesten Stand zu halten. Aus ihr muss der Nachweis hervorgehen, wie das Hochrisiko-KI-System die Anforderungen an solche Systeme erfüllt.[636] Die technische Dokumentation muss so erstellt werden, dass den zuständigen nationalen Behörden und den notifizierten Stellen alle Informationen zur Verfügung stehen, die erforderlich sind, um zu beurteilen, ob das KI-System diese Anforderungen erfüllt. Nicht zugänglich ist die technische Dokumentation hingegen für die von den Hochrisiko-KI-Systemen betroffenen Personen.

ee) Aufzeichnungspflichten

Sehr zu begrüßen sind die in Art. 12 KI-VO geregelten Aufzeichnungspflichten. Hochrisiko-KI-Systeme müssen so konzipiert und entwickelt werden, dass eine automatische Aufzeichnung von Vorgängen und Ereignissen („Protokollierung") während des Betriebs der Hochrisiko-KI-Systeme möglich ist. Dadurch soll gewährleistet werden, dass das Funktionieren des KI-Systems während seines gesamten Lebenszyklus rückverfolgbar ist.[637]

Besondere Anforderungen gelten gem. Art. 12 Abs. 3 KI-VO für die Protokollierungsfunktionen bei biometrischen Fernidentifizierungssystemen. Protokolliert werden muss zumindest: jeder Zeitraum der Verwendung des Systems (Datum und Uhrzeit des Beginns und des Endes jeder Verwendung) (lit. a); die Referenzdatenbank, mit der das System die Eingabedaten abgleicht (lit. b); die Eingabedaten, mit denen die Abfrage zu einer Übereinstimmung geführt hat (lit. c) und die Identität der an der Überprüfung der Ergebnisse beteiligten natürlichen Personen (lit. d). Diese besonderen Anforderungen für biometrische Fernidentifizierungssysteme sind ebenfalls zu begrüßen. Der Zeitpunkt der Verwendung, die zum Abgleich herangezogenen Daten und das verwendete Suchbild sind zentrale Stell-

636 Art. 11 Abs. 1 S. 2 KI-VO.
637 Art. 12 Abs. 1 KI-VO.

schrauben im Gesichtserkennungsprozess.[638] Die Protokollierung der an der Überprüfung der Ergebnisse beteiligten Menschen kann dazu beitragen, dass deren Verantwortung(sgefühl) für diesen Entscheidungsprozess gestärkt wird. Allerdings haben zu diesen Informationen nur die zuständigen Behörden Zugang, nicht die von der Gesichtserkennung betroffenen Personen. Solche Aufzeichnungen legen aber zumindest die Basis für eine Kontrolle, die nicht (wie die zuständigen Behörden) die Rechtskonformität überprüft, sondern Gesichtserkennung spezifisch als Strafverfolgungsmaßnahme auswertet.

ff) Transparenz und Bereitstellung von Informationen für die Betreiber

Art. 13 KI-VO regelt, dass Hochrisiko-KI-Systeme so konzipiert und entwickelt werden müssen, dass ihr Betrieb hinreichend transparent ist, damit die Betreiber die Ergebnisse des Systems angemessen interpretieren und verwenden können.[639] Dies dient laut ErwG 72 dazu, der Undurchsichtigkeit entgegenzuwirken, die bestimmte KI-Systeme für natürliche Personen unverständlich oder zu komplex erscheinen lässt. Im Hinblick auf Gesichtserkennung ist die Undurchsichtigkeit der zugrunde liegenden Algorithmen allerdings weniger problematisch. Zwar können selbst die Entwickler von Gesichtserkennungsalgorithmen die komplexen Rechenoperationen der

638 *Hoffmann*, Der nichtstaatliche Einsatz biometrischer Gesichtserkennungssysteme nach der DSGVO, 2023, 283 weist im Kontext des Einsatzes von Gesichtserkennung durch Private zudem darauf hin, dass die Aufzeichnungspflichten die Betreiber von Gesichtserkennungssystemen dazu anhalten können, die Systeme nur an Orten und zu Zeiten einzusetzen, in denen es ihnen gestattet ist, da ein Verstoß später auffallen und geahndet werden könnte. Für den Einsatz von Gesichtserkennung in der Strafverfolgung zur Identifizierung unbekannter Verdächtiger (also im Nachhinein) gilt dies allerdings nicht, denn zeitliche oder örtliche Beschränkungen gibt es hier nicht. Einen Verstoß gegen Rechtsvorschriften würde es etwa darstellen, wenn die Identität einer Person ermittelt würde, die nicht in Zusammenhang mit einem Strafverfahren steht. Dies ließe sich durch die Protokollierungsfunktion allein aber im Nachhinein nicht feststellen, denn die Information und Tatsache, dass die per Gesichtserkennung gesuchte Person Verdächtige ist, wird außerhalb des KI-Systems generiert (z. B. durch Zeugenaussagen, dass die auf dem Foto abgebildete Person eine Straftat begangen habe).

639 Kritisch zu diesen Vorgaben (zu wenig spezifisch) bereits *Ebers*, in: Colonna/Greenstein, Nordic Yearbook of Law and Informatics 2020, 2022, 103, 130; *Ebers/Hoch/Rosenkranz/Ruschemeier/Steinrötter*, RDi 2021, 528, 533 f. Siehe zu den Vorgaben auch *Kalbhenn*, ZUM 2021, 663, 667 f.

verwendeten künstlichen neuronalen Netze nicht nachvollziehen.[640] Das *Ergebnis* kann ein Mensch aber ohne Weiteres überprüfen und nachvollziehen; er kann die Gesichter der Personen, die das System als übereinstimmend wertet, selbst visuell vergleichen.

Die beim Einsatz von Gesichtserkennung in der Strafverfolgung problematische Intransparenz ist keine *technische* Undurchsichtigkeit. Vielmehr ist es für die Bürger nicht nachvollziehbar, welche Daten wann mit wem für welche Straftat abgeglichen werden. Diese Form der fehlenden Transparenz adressiert die KI-Verordnung nicht.

Und selbst die erwähnte Regelung des Art. 13 KI-VO, die technische Transparenz (soweit möglich) gewährleisten soll, hilft den von Gesichtserkennung betroffenen Personen nicht weiter, denn diese Vorschriften zu Transparenz und Bereitstellung von Informationen gelten nur mit Blick auf die *Betreiber* des KI-Systems. Betreiber ist gem. Art. 3 Nr. 4 KI-VO-E eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System in eigener Verantwortung verwendet. Das sind beim Einsatz von Gesichtserkennung die Polizeibehörde, die das System nutzt, sowie die Polizisten, die das System verwenden. Transparenzpflichten gegenüber den von der Gesichtserkennung Betroffenen regelt die KI-Verordnung nicht.

gg) Menschliche Aufsicht

Nach Art. 14 KI-VO sind Hochrisiko-KI-Systeme so zu konzipieren und zu entwickeln, dass sie während der Dauer der Verwendung von natürlichen Personen wirksam beaufsichtigt werden können.[641] Dies dient nach Art. 14 Abs. 2 KI-VO der Verhinderung oder Minimierung der Risiken für Gesundheit, Sicherheit oder Grundrechte, die entstehen können, wenn ein Hochrisiko-KI-System „im Einklang mit seiner Zweckbestimmung oder im Rahmen einer vernünftigerweise vorhersehbaren Fehlanwendung" verwendet wird.[642] Die menschliche Aufsicht kann durch zwei Arten von Vorkeh-

640 Hierzu Kapitel I. E. III.

641 Zu Recht sehr kritisch zu diesen Vorgaben *Guijarro Santos*, ZfDR 2023, 23, 28 ff.; kritisch auch *Ebers/Hoch/Rosenkranz/Ruschemeier/Steinrötter*, RDi 2021, 528, 533 f.; siehe auch *Geminn*, ZD 2021, 354, 357.

642 *Valta/Vasel*, ZRP 2021, 142, 144 weisen darauf hin, dass für eine effektive Kontrolle häufig hochqualifiziertes, wissenschaftlich ausgebildetes Personal erforderlich ist, „wenn die Anforderungen mehr als Worte bleiben sollen".

rungen gewährleistet werden: entweder durch Vorkehrungen, die vor dem Inverkehrbringen oder der Inbetriebnahme vom Anbieter bestimmt und, sofern technisch machbar, in das Hochrisiko-KI-System eingebaut werden (Art. 14 Abs. 3 lit. a KI-VO), oder durch Vorkehrungen, die vor dem Inverkehrbringen oder der Inbetriebnahme des Hochrisiko-KI-Systems vom Anbieter bestimmt werden und dazu geeignet sind, vom Betreiber umgesetzt zu werden (Art. 14 Abs. 3 lit. b KI-VO).

Für biometrische Fernidentifizierungssysteme stellt Art. 14 Abs. 5 Uabs. 1 KI-VO dahingehend die besondere Anforderung auf, dass diese Vorkehrungen so gestaltet sein müssen, dass der Betreiber keine Maßnahmen oder Entscheidungen allein aufgrund des vom System hervorgebrachten Identifizierungsergebnisses treffen kann, solange dies nicht von „zwei natürlichen Personen, die die notwendige Kompetenz, Ausbildung und Befugnis besitzen, getrennt überprüft und bestätigt wurde". Es ist zu begrüßen, dass – im Gegensatz zum ursprünglichen Entwurf der EU-Kommission – nunmehr die erforderliche Qualifikation dieser natürlichen Personen betont wurde, auch wenn die Formulierung recht allgemein bleibt. (Wann besitzt jemand die „notwendige Kompetenz [und] Ausbildung" um die Ergebnisse eines Gesichtserkennungssystems zu überprüfen?) Auch was eine „getrennte" Überprüfung bedeutet, ist nicht näher geregelt; gemeint sein dürfte (und sinnvoll ist) eine Überprüfung der Ergebnisse durch zwei Personen unabhängig voneinander in dem Sinne, dass dem jeweils anderen das Überprüfungsergebnis des anderen nicht bekannt ist. Laut ErwG 73 könnten diese Personen von einer oder mehreren Einrichtungen stammen und die Person umfassen, die das System bedient oder verwendet. Diese Anforderung, so weiter ErwG 73, sollte „keine unnötigen Belastungen oder Verzögerungen mit sich bringen, und es könnte ausreichen, dass die getrennten Überprüfungen durch die verschiedenen Personen automatisch in die vom System erzeugten Protokolle aufgenommen werden". Nach Art. 14 Abs. 5 Uabs. 2 KI-VO soll die Anforderung einer getrennten Überprüfung durch mindestens zwei natürliche Personen allerdings nicht für Hochrisiko-KI-Systeme gelten, die für Zwecke in den Bereichen Strafverfolgung, Migration, Grenzkontrolle oder Asyl verwendet werden, wenn die Anwendung dieser Anforderung nach Unionsrecht oder nationalem Recht unverhältnismäßig wäre.

Diese besonderen Vorgaben (getrennte Überprüfung und Bestätigung des Identifizierungsergebnisses durch zwei natürliche Personen, die die notwendige Kompetenz, Ausbildung und Befugnis besitzen) klingen zwar zunächst im Kontext biometrischer Fernidentifizierung wie Gesichtserken-

nung sehr sinnvoll. Allerdings ist fraglich, wie diese *technisch* umgesetzt werden sollen, denn um die technische Gestaltung des KI-Systems geht es an dieser Stelle.[643] Bei der Verwendung automatisierter Gesichtserkennung in der Strafverfolgung trifft der Betreiber des Systems zwar eine Entscheidung (er bestätigt oder verwirft eine Personenidentität); allerdings läuft diese – ebenso wie die nachfolgenden Ermittlungsmaßnahmen im Falle einer Identifizierung – gänzlich außerhalb des KI-Systems ab. Wie soll die technische Ausgestaltung des KI-Systems dies verhindern? Zu denken wäre an eine Art Warnhinweis („Dies ist keine eindeutige Identifizierung. Dem System können Fehler unterlaufen. Eine menschliche Überprüfung durch zwei Personen ist erforderlich."). Dies verhindert aber technisch nicht, dass dennoch Maßnahmen oder Entscheidungen ohne eine solche Kontrolle getroffen werden. Erforderlich wäre etwa eine Gestaltung des Systems, die es nur erlaubt, weitere Informationen über die als Verdächtiger identifizierte Person abzurufen und an die Ermittlungsbeamten weiterzuleiten, nachdem zwei verschiedene Menschen sich gegenüber dem System authentifiziert und die Ergebnisse geprüft haben. Erschwerend kommt hinzu, dass das System so ausgestaltet sein soll, dass bei Unverhältnismäßigkeit dann doch keine getrennte Überprüfung durch mindestens zwei natürliche Personen erforderlich sein soll. Diese Unverhältnismäßigkeit ist aber eine *Wertungsentscheidung*, die typischerweise im Einzelfall getroffen werden muss. Soll das System also mit einem Button ausgestattet sein, den der Betreiber (aus technischer Sicht:) nach Belieben anklickt („Hier wäre eine getrennte Überprüfung durch zwei natürliche Personen unverhältnismäßig."), sodass das System dann weitere Maßnahmen ohne eine solche Überprüfung ermöglicht? Wie die Entwickler von Gesichtserkennungssystemen diese Vorgaben technisch umsetzen werden und ob dies dem Zweck der menschlichen Aufsicht gerecht wird, bleibt abzuwarten.

Implizit könnte man aus Art. 14 Abs. 5 KI-VO ableiten, dass die Vorschrift zugleich verbindlich regelt, dass biometrische Fernidentifizierungssysteme nur so *verwendet* werden dürfen, dass eine Entscheidung oder Maßnahme erst nach Überprüfung und Bestätigung des Identifizierungsergebnisses von mindestens zwei natürlichen Personen getroffen wird. Dann wäre zugleich eine Pflicht für die Betreiber des KI-Systems normiert und damit auch Vorgaben für eine nationale Rechtsgrundlage zum Einsatz von Gesichtserkennung. Dagegen spricht jedoch die Verortung dieser Regelung

643 Adressat der Regelung ist der *Anbieter* des KI-Systems, nicht der Betreiber; vgl. auch *Martini*, in: Martini/Wendehorst, KI-VO, Art. 14 Rn. 15, 46.

in Art. 14 Abs. 5 KI-VO in Kapitel III Abschnitt 2 der KI-VO (wo technische Anforderungen an die KI-Systeme geregelt werden) und die Formulierung, die sich auf die Ausgestaltung des Systems bezieht, nicht auf die damit einhergehenden Vorgänge außerhalb des Systems. Allerdings dürfte es aufgrund der Fehleranfälligkeit von Gesichtserkennungsmaßnahmen (siehe hierzu unten Kapitel III. B. II. und III.) zumindest aus rechtspolitischer Sicht sinnvoll sein, eine Pflicht zur getrennten Überprüfung der Treffer durch zwei sachverständige Experten in einer Rechtsgrundlage für den Einsatz automatisierter Gesichtserkennung zu regeln.

hh) Genauigkeit, Robustheit und Cybersicherheit

Zudem müssen nach Art. 15 Abs. 1 KI-VO Hochrisiko-KI-Systeme so konzipiert und entwickelt werden, dass sie ein angemessenes Maß an Genauigkeit, Robustheit und Cybersicherheit erreichen und in dieser Hinsicht während ihres gesamten Lebenszyklus beständig funktionieren. *Hacker/Wessel* kritisieren, dass Art. 10 KI-VO einerseits die Daten und damit den *Prozess* des Modelltrainings regelt, andererseits in Art. 15 KI-VO auch Anforderungen an die *Ergebnisse* stellt (insbesondere muss ein angemessenes Maß an Genauigkeit erreicht werden).[644] Damit komme es zu einer Doppelung von direkter und indirekter Regulierung der Trainingsdaten, da mangelhafte Trainingsdaten zu suboptimalen Ergebnissen führen könnten.[645] Eine Regulierung sowohl des Trainingsprozesses als auch der Ergebnisse kann allerdings sinnvoll sein, denn auch andere Faktoren als die Trainingsdaten können zu einer mangelnden Leistungsfähigkeit eines KI-Systems führen. Bei Gesichtserkennungssystemen hängt die Leistung neben den Trainingsdaten beispielsweise auch entscheidend von der Architektur des verwendeten künstlichen neuronalen Netzes ab. Eine einfache Architektur mit nur wenigen Neuronen wird typischerweise schlechter funktionieren als eine aufwendigere Architektur mit vielen Neuronen, die sinnvoll verknüpft sind. Ein weiterer Faktor für die Erkennungsgenauigkeit eines Gesichtserkennungssystems ist die Strategie, mit der das System trainiert wird (Zielfunktion); auch diese ist von den Trainingsdaten insoweit unabhängig. Insofern ist es sinnvoll, dass zusätzlich zu adäquaten Trainingsdaten gefordert wird, dass auch im Ergebnis ein angemessenes Maß an Genauigkeit erreicht

644 *Hacker/Wessel,* in: BMUV/Rostalski, Künstliche Intelligenz, 2022, 53, 63 f.
645 *Hacker/Wessel,* in: BMUV/Rostalski, Künstliche Intelligenz, 2022, 53, 64.

werden muss. In ihrer Forderung, dass Prozessregulierung und Ergebnisregulierung besser aufeinander abgestimmt sein sollten,[646] ist *Hacker/Wessel* jedoch zuzustimmen.

Unklar bleibt, was ein „angemessenes Maß" an Genauigkeit ist. Um die technischen Aspekte der Art und Weise der Messung des angemessenen Maßes an Genauigkeit näher zu bestimmen, soll die Kommission nach Art. 15 Abs. 2 KI-VO (vgl. auch ErwG 74 S. 6 und 7) in Zusammenarbeit mit einschlägigen Interessenträgern und Organisationen wie Metrologie- und Benchmarking-Behörden gegebenenfalls die Entwicklung von Benchmarks und Messmethoden fördern. Faktisch wird damit die Entscheidung, welche Anforderungen an die Genauigkeit von KI-Systemen zu stellen sind, an diese Normierungsinstitutionen übertragen. Sie entscheiden damit auch, mit den Worten *Martinis* gesprochen, inwiefern „die Einzelfallgerechtigkeit der Genauigkeit eines KI-Systems geopfert werden darf – oder ob die allgemeine Genauigkeit zugunsten Einzelner zu reduzieren ist".[647] Wann ein „angemessenes Maß" an Genauigkeit vorliegt, ist keine rein technische Frage, sondern enthält Wertentscheidungen. Insbesondere besteht regelmäßig ein inhärenter Trade-off zwischen Genauigkeit und Fairness[648] eines KI-Systems.[649] Auch kann ein System zwar insgesamt einen hohen Genauigkeitsgrad aufweisen, für einzelne Subgruppen aber dennoch sehr fehlerhaft sein.

ii) Registrierung

Nach Art. 49 Abs. 1 KI-VO hat der Anbieter (oder ggf. sein Bevollmächtigter[650]) vor dem Inverkehrbringen oder der Inbetriebnahme eines in Anhang III aufgeführten Hochrisiko-KI-Systems sich und Informationen

646 *Hacker/Wessel,* in: BMUV/Rostalski, Künstliche Intelligenz, 2022, 53, 64.

647 *Martini*, in: Martini/Wendehorst, KI-VO, Art. 15 Rn. 37; vgl. auch *Guijarro Santos*, ZfDR 2023, 23, 33 f.

648 Wobei auch die Definition von „Fairness" sowohl in der Informatik als auch in der Rechtswissenschaft hoch umstritten und längst nicht geklärt ist.

649 Siehe nur *Kleinberg/Mullainathan/Raghavan*, 8th Innovations in Theoretical Computer Science Conference (ITCS 2017), Leibniz International Proceedings in Informatics (LIPIcs), Vol. 67, 2017, 1.

650 Vgl. Art. 3 Nr. 5 KI-VO; danach ist Bevollmächtigter „eine in der Union ansässige oder niedergelassene natürliche oder juristische Person, die vom Anbieter eines KI-Systems oder eines KI-Modells mit allgemeinem Verwendungszweck schriftlich dazu bevollmächtigt wurde und sich damit einverstanden erklärt hat, in seinem

über sein System in einer von der Kommission einzurichtenden und zu verwaltenden EU-Datenbank (Art. 71 KI-VO) zu registrieren; hierzu zählen auch biometrische Fernidentifizierungssysteme (Anhang III Nr. 1). Speziell bei biometrischen Fernidentifizierungssystemen, die in der Strafverfolgung (sowie im Bereich Migration, Asyl und Grenzkontrolle) eingesetzt werden, erfolgt die Registrierung gem. Art. 49 Abs. 4 KI-VO in einem sicheren nicht öffentlichen Teil dieser EU-Datenbank; zudem müssen weniger Informationen bereitgestellt werden als bei anderen Hochrisiko-KI-Systemen[651].

jj) Marktüberwachung

Die KI-Verordnung regelt auch eine Aufsichtsstruktur.[652] Sie richtet ein Europäisches Gremium für Künstliche Intelligenz (KI-Gremium; vgl. Art. 65 Abs. 1 KI-VO) ein, das gem. Art. 66 Abs. 1 KI-VO die Kommission und die Mitgliedstaaten berät und unterstützt, um die einheitliche und wirksame Anwendung der KI-Verordnung zu erleichtern. Auch ein Europäisches Büro für Künstliche Intelligenz (Art. 3 Nr. 47 und Art. 64 KI-VO) als Bestandteil der EU-Kommission wird geschaffen; über dieses Büro entwickelt die Kommission die Sachkenntnis und Fähigkeiten der Union auf dem Gebiet der KI. Zuständig für die tatsächliche Aufsicht sind grundsätzlich die nationalen Aufsichtsbehörden; diese werden nach Art. 70 Abs. 1 KI-VO von den Mitgliedstaaten eingerichtet oder benannt. Die aufsichtsrechtlichen Befugnisse nimmt eine (von dem Mitgliedstaat einzurichtende oder zu benennende) Marktüberwachungsbehörde[653] wahr.

Für die Überwachung des Einsatzes biometrischer Fernidentifizierungssysteme in der Strafverfolgung benennen die Mitgliedstaaten gem. Art. 74 Abs. 8 KI-VO die Datenschutzbehörden. Diese sollen über „wirksame Ermittlungs- und Korrekturbefugnisse verfügen, einschließlich mindestens der Befugnis, Zugang zu allen personenbezogenen Daten, die verarbeitet werden, und zu allen Informationen, die für die Ausübung ihrer Aufgaben erforderlich sind, zu erhalten" (ErwG 159). Ihnen soll es außerdem möglich sein, ihre Befugnisse in „völliger Unabhängigkeit" auszuüben. Dies schließt,

Namen die in dieser Verordnung festgelegten Pflichten zu erfüllen bzw. Verfahren durchzuführen".

651 Vgl. auch Art. 60 Abs. 4 lit. c KI-VO; Anhang VIII Abschnitt A Nr. 12 Hs. 2 KI-VO.

652 Sehr instruktiv *Martini/Botta*, MMR 2024, 630.

653 Definition in Art. 3 Nr. 26 KI-VO.

worauf *Martini/Botta* zu Recht hinweisen, eine staatliche Fach-, Rechts- und Dienstaufsicht aus.[654]

kk) Pflichten der Betreiber

Wie bereits angesprochen, ist Betreiber eines KI-Systems gem. Art. 3 Nr. 4 KI-VO eine natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System in eigener Verantwortung verwendet. Beim Einsatz von Gesichtserkennung ist Betreiber daher jedenfalls die Polizeibehörde, die das System nutzt. Auch die Polizistin, die das System bedient bzw. verwendet, dürfte als natürliche Person unter den Begriff des Betreibers fallen. Allerdings spricht Art. 26 Abs. 2 KI-VO davon, dass die Betreiber „natürlichen Personen, die über die erforderliche Kompetenz, Ausbildung und Befugnis verfügen, die menschliche Aufsicht [übertragen] und […] ihnen die erforderliche Unterstützung zukommen" lassen sollen; das würde bedeuten, dass jedenfalls die natürliche Person, die die menschliche Aufsicht gewährleistet (bei Gesichtserkennung insbesondere: Überprüfung des Identifizierungsergebnisses), nicht – jedenfalls nicht allein deshalb – Betreiber ist.[655]

Für die Betreiber von Hochrisiko-KI-Systemen sieht die KI-Verordnung vergleichsweise wenige Pflichten vor.[656] Sie müssen insbesondere „geeignete technische und organisatorische Maßnahmen [treffen], um sicherzustellen, dass sie solche Systeme entsprechend der den Systemen beigefügten Betriebsanleitungen" verwenden (Art. 26 Abs. 1 KI-VO) und den Betrieb des Hochrisiko-KI-Systems überwachen (Art. 26 Abs. 5 KI-VO). Zudem haben sie nach Art. 26 Abs. 4 KI-VO dafür zu sorgen, dass die Eingabedaten der Zweckbestimmung des Systems entsprechen. Relevant ist auch die Vor-

654 *Martini/Botta*, MMR 2024, 630, 632.

655 Auch Art. 14 Abs. 5 Uabs. 1 KI-VO deutet darauf hin, dass die Person, die das Gesichtserkennungssystem bedient bzw. verwendet (im Sinne von: Foto eines Verdächtigen hochladen) Betreiber ist und dieser jedoch nicht zwingend die menschliche Aufsicht ist: „Bei den in Anhang III Nummer 1 Buchstabe a genannten Hochrisiko-KI-Systemen müssen die in Absatz 3 des vorliegenden Artikels genannten Vorkehrungen so gestaltet sein, dass außerdem der *Betreiber* keine Maßnahmen oder Entscheidungen allein aufgrund des vom System hervorgebrachten Identifizierungsergebnisses trifft, solange diese Identifizierung nicht von mindestens zwei natürlichen Personen, die die notwendige Kompetenz, Ausbildung und Befugnis besitzen, getrennt überprüft und bestätigt wurde." (Hervorhebung J. H.).

656 Zu den Pflichten auch bereits *Roos/Weitz*, MMR 2021, 844, 849.

gabe, dass die Betreiber die von den Hochrisiko-KI-Systemen erzeugten Protokolle aufbewahren müssen (Art. 26 Abs. 6 KI-VO), jedenfalls „soweit diese Protokolle ihrer Kontrolle unterliegen". Die Protokolle werden für einen der Zweckbestimmung des Hochrisiko-KI-Systems angemessenen Zeitraum von mindestens sechs Monaten aufbewahrt, sofern im geltenden Unionsrecht, insbesondere im Unionsrecht über den Schutz personenbezogener Daten, oder im geltenden nationalen Recht nichts anderes bestimmt ist.

Handelt es sich bei dem Betreiber des Hochrisiko-KI-Systems um eine Einrichtung des öffentlichen Rechts – darunter fallen Polizeibehörden –, dann hat er gem. Art. 27 Abs. 1 KI-VO vor der Inbetriebnahme des Systems eine Abschätzung der Auswirkungen vorzunehmen, die die Verwendung eines solchen Systems auf die Grundrechte haben kann (Grundrechte-Folgenabschätzung bzw. Fundamental rights impact assessment). Diese umfasst gem. Art. 27 Abs. 1 KI-VO eine Beschreibung der Verfahren des Betreibers, bei denen das Hochrisiko-KI-System im Einklang mit seiner Zweckbestimmung verwendet wird (lit. a), eine Beschreibung des Zeitraums und der Häufigkeit, innerhalb dessen bzw. mit der jedes Hochrisiko-KI-System verwendet werden soll (lit. b), die Kategorien der natürlichen Personen und Personengruppen, die von seiner Verwendung im spezifischen Kontext betroffen sein könnten (lit. c), die spezifischen Schadensrisiken, die sich auf die ermittelten Kategorien natürlicher Personen oder Personengruppen auswirken könnten, unter Berücksichtigung der vom Anbieter bereitgestellten Informationen (lit. d), eine Beschreibung der Umsetzung von Maßnahmen der menschlichen Aufsicht entsprechend den Betriebsanleitungen (lit. e) sowie die Maßnahmen, die im Falle des Eintretens dieser Risiken zu ergreifen sind, einschließlich der Regelungen für die interne Unternehmensführung und Beschwerdemechanismen (lit. f). Die Ergebnisse dieser Grundrechte-Folgenabschätzung teilt der Betreiber der Marktüberwachungsbehörde mit (Art. 27 Abs. 3 KI-VO).

In der Literatur wird kritisiert, dass der Mehrwert dieser rein grundrechtsbezogenen Risikofolgenabschätzung gegenüber der allgemeinen Risikobewertung nach Art. 9 KI-VO unklar sei.[657] Für den Bereich der Strafverfolgung kommt hinzu, dass die JI-RL in Art. 27 eine Datenschutz-Folgenab-

657 *Chibanguza/Steege*, NJW 2024, 1769, 1772; kritisch auch *Hacker,* Comments on the Final Trilogue Version of the AI Act, 2024, 11 und bereits zum Entwurf einer KI-Verordnung (in der eine Grundrechte-Folgenabschätzung noch auch für private Akteure vorgesehen war) *Hacker/Berz*, ZRP 2023, 226, 228.

schätzung vorsieht; enthalten muss sie gem. Art. 27 Abs. 2 JI-RL „zumindest eine allgemeine Beschreibung der geplanten Verarbeitungsvorgänge und eine Bewertung der in Bezug auf die Rechte und Freiheiten der betroffenen Personen bestehenden Risiken sowie der geplanten Abhilfemaßnahmen, Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Richtlinie eingehalten wird". Die KI-Verordnung sieht vor, dass die Grundrechte-Folgenabschätzung diese Datenschutz-Folgenabschätzung nach der JI-Richtlinie ergänzen soll (Art. 27 Abs. 4 KI-VO). Gegenüber der allgemeinen Risikobewertung nach Art. 9 KI-VO und gegenüber der Datenschutz-Folgenabschätzung nach Art. 27 JI-RL ist die Grundrechte-Folgenabschätzung nach der KI-Verordnung aber zumindest etwas spezifischer, da etwa auch Informationen über die Häufigkeit der Verwendung des KI-Systems und eine Beschreibung der Umsetzung von Maßnahmen der menschlichen Aufsicht geliefert und bedacht werden müssen.

c) Keine Benachrichtigungspflicht und kaum subjektive Rechte

Nicht geregelt sind Mitteilungspflichten mit Blick auf die von den Hochrisiko-KI-Systemen betroffenen Personen. Sie müssen daher nach der KI-Verordnung auch nicht darüber informiert werden, dass sie per biometrischer Fernidentifizierung identifiziert wurden. Insbesondere ergibt sich eine Benachrichtigungspflicht nicht aus Art. 50 KI-VO, der Transparenzpflichten für die Anbieter und Betreiber bestimmter KI-Systeme regelt. Eine Benachrichtigungspflicht nach Art. 50 Abs. 1 KI-VO scheidet aus, weil es sich bei Gesichtserkennungssystemen nicht um KI-Systeme handelt, die – jedenfalls mit Blick auf die Betroffenen – für die direkte Interaktion mit natürlichen Personen bestimmt sind. Ohnehin besteht nach Art. 50 Abs. 1 S. 2 KI-VO diese Pflicht nicht für gesetzlich zur Aufdeckung, Verhütung, Ermittlung oder Verfolgung von Straftaten zugelassene KI-Systeme, wenn geeignete Schutzvorkehrungen für die Rechte und Freiheiten Dritter bestehen. Auch aus Art. 26 Abs. 11 KI-VO folgt keine Benachrichtigungspflicht. Nach dieser Vorschrift haben zwar die Betreiber der in Anhang III aufgeführten Hochrisiko-KI-Systeme, die natürliche Personen betreffende Entscheidungen treffen oder bei solchen Entscheidungen Unterstützung leisten (dazu gehört automatisierte Gesichtserkennung), die natürlichen Personen darüber zu

informieren, dass sie der Verwendung des Hochrisiko-KI-Systems unterliegen. Zwar soll gemäß Art. 26 Abs. 11 S. 2 KI-VO für Hochrisiko-KI-Systeme, die zu Strafverfolgungszwecken verwendet werden, Art. 13 JI-RL gelten, der Informationspflichten statuiert. Allerdings regelt Art. 13 JI-RL keine individuelle Benachrichtigungspflicht (z. B. Benachrichtigung des Beschuldigten), sondern eine allgemeine Informationspflicht, der – so ausdrücklich ErwG 42 der JI-RL – auch genügt ist, wenn die Informationen auf der Website der zuständigen Behörde bereitgestellt werden.[658]

Auch verleiht die KI-Verordnung keine starken individuellen Rechte, insbesondere kein Recht auf Einsicht in die protokollierten Vorgänge bei der Verwendung biometrischer Fernidentifizierung zur Strafverfolgung.[659]

d) Spezifische Vorgaben für die Identitätsermittlung per nachträglicher biometrischer Fernidentifizierung?

Für die in dieser Arbeit vorrangig untersuchte Einsatzvariante der Identitätsermittlung finden sich in der KI-Verordnung kaum konkrete spezifische Vorgaben.

aa) Kein Genehmigungsvorbehalt

Insbesondere regelt die KI-Verordnung für dieses Einsatzszenario keinen Richter- oder sonstigen Genehmigungsbehalt. Grundsätzlich sieht die KI-Verordnung zwar sowohl für die (ausnahmsweise erlaubte) Verwendung biometrischer Echtzeit-Fernidentifizierung in der Strafverfolgung als auch

658 Zur Unterscheidung zwischen Benachrichtigungspflichten nach der StPO und der Informationspflicht nach Art. 13 JI-RL, § 55 BDSG auch *Schindler*, Biometrische Videoüberwachung, 2021, 710 f. Näher zu Art. 13 JI-RL und seiner Umsetzung in § 55 BDSG siehe etwa Kühling/Buchner/*Schwichtenberg*, 4. Aufl. 2024, BDSG § 55 Rn. 2 ff.; BeckOK DatenschutzR/*Schild*, 46. Ed., Stand: 1.11.2023, BDSG § 55 Rn. 6; Paal/Pauly/Paal, 3. Aufl. 2021, BDSG § 55 Rn. 1 ff. Zu § 56 BDSG ausführlich *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, 2023, 542 ff.

659 Vgl. auch *Hoffmann*, Der nichtstaatliche Einsatz biometrischer Gesichtserkennungssysteme nach der DSGVO, 2023, 273; *Hoffmann*, K&R 2021, 369 (370); anders *Floridi*, Philosophy & Technology 2021, 215, 216. Es wurde lediglich – sehr spät im Gesetzgebungsprozess – noch mit Art. 86 KI-VO ein „Recht auf Erläuterung der Entscheidungsfindung im Einzelfall eingeführt", wobei dessen Reichweite und „Schlagkraft" noch äußerst fraglich sind.

für die anderen Einsatzvarianten einen Genehmigungsvorbehalt vor. Nach Art. 26 Abs. 10 S. 1 KI-VO hat der Betreiber eines Hochrisiko-KI-Systems zur nachträglichen biometrischen Fernfernidentifizierung im Rahmen von Ermittlungen zur gezielten Suche einer Person, die der Begehung einer Straftat verdächtigt wird oder aufgrund einer solchen verurteilt wurde, vorab oder unverzüglich, spätestens jedoch binnen 48 Stunden bei einer Justizbehörde oder einer Verwaltungsbehörde, deren Entscheidung bindend ist und einer justiziellen Überprüfung unterliegt, die Genehmigung für die Nutzung dieses Systems zu beantragen.[660] Ob eine Überprüfung durch eine (formal) unabhängige Verwaltungsbehörde tatsächlich in jedem Mitgliedstaat ein echtes Gegengewicht zu den Strafverfolgungsbehörden darstellt und Gewaltenteilung gewährleisten kann, ist fraglich.[661]

Für den in dieser Arbeit vorrangig untersuchten Einsatz automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger kommt es auf die nähere Ausgestaltung dieser Vorgaben der KI-Verordnung allerdings nicht an. Denn der Genehmigungsvorbehalt gilt ausdrücklich *nicht* bei der Verwendung biometrischer Fernidentifizierung „zur erstmaligen Identifizierung eines potenziellen Verdächtigen auf der Grundlage objektiver und nachprüfbarer Tatsachen, die in unmittelbarem Zusammenhang mit der Straftat stehen" (Art. 26 Abs. 10 S. 1 aE KI-VO).

bb) Keine echten materiellen Vorgaben

Echte materielle Vorgaben liefert die KI-Verordnung für den Einsatz automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger nicht.

Insbesondere hat sich nicht die Position des EU-Parlaments durchgesetzt, nach der die Verwendung biometrischer Fernidentifizierung zur Analyse von aufgezeichnetem Bildmaterial öffentlich zugänglicher Räume auf *schwere* Straftaten beschränkt werden sollte (Abänderung 227 der Abänderungen des EU-Parlaments zum Entwurf einer KI-Verordnung der EU-Kommission). Nach diesem Vorschlag hätte gem. Art. 5 Abs. 1 lit. dd verboten sein sollen: „die Inbetriebnahme oder Nutzung von KI-Systemen zur

660 Für die Echtzeit-Fernidentifizierung zu Strafverfolgungszwecken in öffentlich zugänglichen Räumen ist in Art. 5 Abs. 3 KI-VO ein ähnlicher Genehmigungsvorbehalt vorgeschrieben.

661 Vgl. auch *Hacker,* Comments on the Final Trilogue Version of the AI Act, 2024, 7.

Analyse von aufgezeichnetem Bildmaterial öffentlich zugänglicher Räume durch Systeme zur nachträglichen biometrischen Fernidentifizierung, es sei denn, sie unterliegen einer vorgerichtlichen Genehmigung im Einklang mit dem Unionsrecht und sind für die gezielte Fahndung im Zusammenhang mit einer bestimmten schweren Straftat im Sinne von Artikel 83 Absatz 1 AEUV, die bereits zum Zweck der Strafverfolgung stattgefunden hat, unbedingt erforderlich".[662] Diese Beschränkung des Einsatzes nachträglicher biometrischer Fernidentifizierung auf schwere Straftaten findet sich nicht in der finalen Fassung der KI-Verordnung.

Art. 26 Abs. 10 Uabs. 3 S. 1 KI-VO legt fest, dass in „keinem Fall […] ein solches Hochrisiko-KI-System zur nachträglichen biometrischen Fernidentifizierung zu Strafverfolgungszwecken in nicht zielgerichteter Weise und ohne jeglichen Zusammenhang mit einer Straftat, einem Strafverfahren, einer tatsächlichen und bestehenden oder tatsächlichen und vorhersehbaren Gefahr einer Straftat oder der Suche nach einer bestimmten vermissten Person verwendet werden" darf. Dass eine Strafverfolgungsmaßnahme nicht ohne den Anlass einer Straftat ergriffen werden darf, ist für das deutsche Strafprozessrecht allerdings nichts Neues.

Wenig konkret[663] postuliert zudem ErwG 95 drei „Vorgaben" für den Einsatz nachträglicher biometrischer Fernidentifizierung (die aber ohnehin nur als „Soll"-Vorgaben formuliert sind):

Die Verwendung von Systemen zur nachträglichen biometrischen Fernidentifizierung solle in Anbetracht des intrusiven Charakters von Systemen zur nachträglichen biometrischen Fernidentifizierung „Schutzvorkehrungen unterliegen." Davon abgesehen, dass diese Vorgabe lediglich an einer einzigen Stelle und noch dazu in einem Erwägungsgrund statt in einer Vorschrift genannt wird:[664] Wie diese Schutzvorkehrungen aussehen könnten, wird nicht einmal katalogartig angedeutet. Hier liegt es also an den Mitgliedstaaten, geeignete Schutzvorkehrungen zu schaffen, wobei zu

662 Zunächst schien es so, als ob dieser Vorschlag sich in der finalen Fassung der KI-Verordnung durchgesetzt habe. Einer Pressemitteilung des EU-Parlaments zufolge wurde in den Verhandlungen mit Blick auf biometrische Fernidentifizierung festgehalten: „Negotiators agreed on a series of safeguards and narrow exceptions for the use of biometric identification systems (RBI) in publicly accessible spaces for law enforcement purposes, subject to prior judicial authorisation and for strictly defined lists of crime. ‚Post-remote' RBI would be used strictly in the targeted search of a person convicted or suspected of having committed a serious crime." (*EU-Parlament*, Pressemitteilung v. 9.12.2023, https://perma.cc/2UEL-4A8Y).

663 Siehe auch *Hacker,* Comments on the Final Trilogue Version of the AI Act, 2024, 8.

664 Anders etwa Art. 10, Art. 11 Abs. 2 und 3, Art. 37 Abs. 1 lit. a, Art. 40 lit. b JI-RL.

hoffen ist, dass sie diese vage in einem Erwägungsgrund „versteckte" Vorgabe überhaupt zur Kenntnis nehmen.

Weiterhin sollen Systeme zur nachträglichen biometrischen Fernidentifizierung, so ErwG 95, „stets auf verhältnismäßige, legitime und unbedingt erforderliche Weise eingesetzt werden und somit zielgerichtet sein, was die zu identifizierenden Personen, den Ort und den zeitlichen Anwendungsbereich betrifft, und auf einem geschlossenen Datensatz rechtmäßig erworbener Videoaufnahmen basieren". Auch diese „Soll"-Vorgaben bringen wenig Neues. Dass eine Strafverfolgungsmaßnahme legitim, zielgerichtet und verhältnismäßig sein muss, ergibt sich bereits aus dem Verfassungsrecht. Dasselbe gilt für die Vorgabe, dass Systeme zur nachträglichen biometrischen Fernidentifizierung im Rahmen der Strafverfolgung nicht so verwendet werden dürfen, dass sie zu „willkürlicher Überwachung" führen. Was „unbedingt erforderlich" (ErwG 95) bedeutet, ist bereits mit Blick auf dieselbe Formulierung in der JI-Richtlinie umstritten, auch und gerade bei der Verarbeitung biometrischer Daten (Art. 10 JI-RL);[665] hierzu sogleich unten Kapitel II. B. I. 2. b). Bei dem Passus, dass die biometrische Fernidentifizierung „auf einem geschlossenen Datensatz rechtmäßig erworbener Videoaufnahmen basieren" soll, fällt auf, dass es dabei ausdrücklich nicht darum geht, dass die Videoaufzeichnungen als solche rechtmäßig waren; vielmehr soll nur der Erwerb dieser durch die Strafverfolgungsbehörden rechtmäßig sein.[666]

Außerdem sollen die Vorgaben für die nachträgliche biometrische Fernidentifizierung keine Grundlage dafür bieten, das „Verbot" und die „strengen Ausnahmen" für biometrische Echtzeit-Fernidentifizierung zu umgehen (ErwG 95). Hierfür ergeben sich mit Blick auf die in dieser Arbeit vorrangig untersuchte Einsatzvariante keine konkreten Vorgaben.

cc) Keine Entscheidung mit nachteiliger Rechtsfolge ausschließlich auf Grundlage eines Treffers

Zudem muss nach Art. 26 Abs. 10 Uabs. 3 S. 2 KI-VO „sichergestellt werden, dass die Strafverfolgungsbehörden keine ausschließlich auf der Grundlage der Ausgabe solcher Systeme zur nachträglichen biometrischen Fernidenti-

665 Hierzu *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, 2023, 537 f. mwN.
666 So auch die englische Textfassung „legally acquired video footage".

fizierung beruhende Entscheidung, aus der sich eine nachteilige Rechtsfolge für eine Person ergibt, treffen". Hierbei stellen sich mehrere Fragen.

Unklar ist zunächst das Verhältnis zu Art. 14 Abs. 5 KI-VO, der Vorgaben für die menschliche Aufsicht von Hochrisiko-KI-Systemen macht. Dieser sieht bereits ausdrücklich vor, dass bei biometrischen Fernidentifizierungssystemen die Vorkehrungen zur menschlichen Aufsicht so gestaltet sein müssen, dass „der Betreiber keine Maßnahmen oder Entscheidungen allein aufgrund des vom System hervorgebrachten Identifizierungsergebnisses trifft, solange diese Identifizierung nicht von mindestens zwei natürlichen Personen, die die notwendige Kompetenz, Ausbildung und Befugnis besitzen, getrennt überprüft und bestätigt wurde".

Auf den ersten Blick könnte man denken, dass Art. 26 Abs. 10 Uabs. 3 S. 2 KI-VO eine lex specialis Vorschrift zu Art. 14 Abs. 5 KI-VO sei. Denn Art. 14 Abs. 5 KI-VO trifft Regelungen zur menschlichen Aufsicht bei den in Anhang III Nr. 1 lit. a genannten Hochrisiko-KI-Systemen (biometrische Fernidentifizierungssysteme); dazu zählen sowohl Echtzeit- als auch nachträgliche Fernidentifizierungssysteme, und es werden alle biometrischen Fernidentifizierungssysteme erfasst, ungeachtet dessen, in welchem Bereich sie verwendet werden (z. B. Strafverfolgung, Migration, Grenzkontrolle, aber auch kommerzielle Verwendung durch private Unternehmen). Da Art. 26 Abs. 10 Uabs. 3 S. 2 KI-VO sich allein auf Systeme zur nachträglichen Fernidentifizierung im Bereich der Strafverfolgung bezieht, könnte die Vorschrift spezieller sein. Allerdings erwähnt Art. 14 Abs. 5 Uabs. 2 KI-VO den Bereich der Strafverfolgung ausdrücklich.

Gegen eine Einordnung des Art. 26 Abs. 10 Uabs. 3 S. 2 KI-VO als lex specialis Regelung spricht auch, dass die Stoßrichtung jeweils eine andere ist. Art. 14 Abs. 5 KI-VO legt Vorgaben für die *technische* Ausgestaltung von biometrischen Fernidentifizierungssystemen fest; Adressat ist der Anbieter des KI-Systems, nicht der Betreiber.[667] Dagegen dürfte Art. 26 Abs. 10 Uabs. 3 S. 2 KI-VO als eine direkte Regelung (oder zumindest ein an die Mitgliedstaaten gerichteter Regelungsauftrag) zu verstehen sein, die unmittelbar die Ermächtigungsgrundlage zum Einsatz automatisierter Gesichtserkennung ausgestaltet. Art. 26 Abs. 10 Uabs. 3 S. 2 KI-VO und Art. 14 Abs. 5 KI-VO sind daher beide nebeneinander anzuwenden.

Unklar ist weiterhin, was es bedeutet, sicherzustellen, „dass die Strafverfolgungsbehörden keine ausschließlich auf der Grundlage der Ausgabe

667 Kapitel II. B. I. 1. b) gg).

solcher Systeme zur nachträglichen biometrischen Fernidentifizierung beruhende Entscheidung, aus der sich eine nachteilige Rechtsfolge für eine Person ergibt, treffen". Erstens: Wann ist im Strafverfahren von einer „nachteiligen Rechtsfolge" – statt einer hier dem Wortlaut nach nicht ausreichenden „erheblichen Beeinträchtigung" – auszugehen?[668] Eine nachteilige Rechtsfolge ist im Strafverfahren jedenfalls zu bejahen bei der Anklageerhebung (§ 170 Abs. 1 StPO), der Eröffnung des Hauptverfahrens (§ 203 StPO), bei einer Verurteilung, bei Erlass eines Strafbefehls (§§ 407 ff. StPO) und wohl jedenfalls bei den Einstellungen, die mit nachteiligen Rechtsfolgen einhergehen (z. B. Geldauflage bei § 153a StPO).[669] Auch die Anordnung von grundrechtseingreifenden Ermittlungsmaßnahmen stellt eine nachteilige Rechtsfolge dar,[670] da dem Betroffenen insoweit eine Duldungspflicht auferlegt wird.

Zweitens stellt sich die Frage: Wann beruht eine Entscheidung „ausschließlich" auf der Grundlage des biometrischen Fernidentifizierungssystems („decision […] based solely on the output of such post-remote biometric identification systems")? Geht es darum, wie stark und auf welche Weise ein Mensch involviert war, sodass die Entscheidung nicht mehr ausschließlich auf dem System beruht? Art. 26 Abs. 10 Uabs. 3 S. 2 KI-VO könnte aber auch anders zu verstehen sein, nämlich so, dass neben dem Identifizierungsergebnis des biometrischen Fernidentifizierungssystems (unabhängig davon, ob dieses durch einen Menschen bestätigt

668 Zur Unterscheidung zwischen nachteiliger Rechtsfolge einerseits und erheblicher Beeinträchtigung andererseits mit Blick auf die JI-Richtlinie überzeugend *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, 2023, 569 f.

669 So auch zu Art. 11 JI-RL, § 54 BDSG *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, 2023, 569.

670 So auch mit Blick auf Art. 11 Abs. 1, 2 JI-RL *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, 2023, 569; etwas weiter (ebenfalls zu Art. 11 JI-RL) wohl *Golla*, NJW 2021, 667, 672 Fn. 53 („Die Annahme eines Tatverdachts und die darauf beruhende Einleitung eines Ermittlungsverfahren[s] dürfte jedenfalls als nachteilige Rechtsfolge anzusehen sein."); vgl. auch *Golla*, in: Chibanguza/Kuß/Steege, Künstliche Intelligenz, 2022, 2. Teil: § 9 A. KI-Einsatz bei der Polizei Rn. 13. Siehe außerdem *Martini*, der in polizeilichen Maßnahmen wohl (zumindest) eine erhebliche Beeinträchtigung sieht, *Martini*, NVwZ-Extra 1-2/2022, 1, 5: Gesichtserkennungssoftware „trifft immerhin aber auf der Grundlage des Abgleichs mit einer Datenbank automatisiert die Entscheidung darüber, ob eine Person auszusondern ist und sich deshalb polizeiliche Maßnahmen anschließen. Alleine diese Aussonderungsentscheidung kann in Ausnahmefällen bereits eine erhebliche beeinträchtigende Wirkung hervorrufen, die den Tatbestand des Art. 11 JI-RL aktiviert."; vgl. auch Paal/Pauly/*Martini*, 3. Aufl. 2021, DSGVO Art. 22 Rn. 16a.

wurde) noch *weitere Hinweise* auf die Täterschaft des Identifizierten (z. B. Anwesenheit am Tatort) vorliegen müssen. Für ein solches Verständnis würde auch sprechen, dass auch die Bestätigung eines Treffers durch einen Menschen die Entscheidung weiterhin „auf der Grundlage" („based on") des biometrischen Fernidentifizierungssystems erfolgt. Eine ähnliche Vorgabe haben (zumindest auf dem Papier) auch alle US-amerikanischen Strafverfolgungsbehörden, die ihre internen Regelungen veröffentlicht haben und darin vorsehen, dass ein Gesichtserkennungstreffer *allein* kein hinreichender Grund für eine Festnahme sein kann; es müssen weitere Hinweise hinzukommen.[671]

Gegen ein solches Verständnis des Art. 26 Abs. 10 Uabs. 3 S. 2 KI-VO (neben Gesichtserkennungstreffer und dessen Bestätigung durch Menschen sind weitere Hinweise erforderlich) spricht allerdings, dass weitere Hinweise für die Täterschaft des Identifizierten typischerweise gerade erst noch durch weitere Ermittlungsmaßnahmen erlangt werden können. Solche – regelmäßig grundrechtseingreifenden – Ermittlungsmaßnahmen dürften aber gar nicht erst angeordnet werden, wenn man Art. 26 Abs. 10 Uabs. 3 S. 2 KI-VO so liest, dass hierfür zunächst weitere Hinweise auf die Täterschaft vorliegen müssen. Insofern besteht auch ein Unterschied des Art. 26 Abs. 10 Uabs. 3 S. 2 KI-VO zu den Regelungen der US-amerikanischen Strafverfolgungsbehörden; letztere sehen nur vor, dass keine *Festnahme* allein auf Basis eines Gesichtserkennungstreffers erfolgen darf, weitere Ermittlungen hingegen schon. Auch spricht gegen ein solches Verständnis des Art. 26 Abs. 10 Uabs. 3 S. 2 KI-VO (neben Gesichtserkennungstreffer und dessen Bestätigung durch Menschen sind weitere Hinweise erforderlich), dass sich eine ähnliche Formulierung („decision based solely on") in Art. 11 JI-RL findet, bei dem es zweifellos darum geht, wann automatisierte Entscheidungsfindung ohne menschliche Beteiligung zulässig ist. Die vergleichbare Formulierung in Art. 26 Abs. 10 Uabs. 3 S. 2 KI-VO deutet darauf hin, dass hier ebenfalls die Frage der Involvierung von Menschen adressiert werden sollte. Es ist daher davon auszugehen, dass Art. 26 Abs. 10

671 Siehe etwa NYPD, Questions and Answers Facial Recognition, https://perma.cc/S7YN-8H52; Michigan State Police, Facial Recognition – Frequently Asked Questions, https://perma.cc/7CNC-BRVR („It is an investigative lead only, requiring the investigator to continue the criminal investigation before making any final determinations, up to and including arrest.").

Uabs. 3 S. 2 KI-VO vor einer automatisierten Entscheidungsfindung ohne menschliche Beteiligung schützen soll.[672]

Anschließend ist zudem zu klären, wann bei einem solchen Verständnis (wenn ein Gesichtserkennungstreffer durch einen Menschen bestätigt wurde, beruhen weitere Entscheidungen nicht mehr ausschließlich auf dem Gesichtserkennungstreffer) eine Entscheidung ausschließlich auf Grundlage des Fernidentifizierungssystems erfolgt und wann nicht, welche *Anforderungen* also *an die menschliche Beteiligung* zu stellen sind. Hier kann an die Überlegungen in der Literatur zu Art. 11 JI-RL (automatisierte Entscheidungsfindung im Einzelfall) angeknüpft werden.[673] Danach ist eine Entscheidung jedenfalls dann ausschließlich automatisiert getroffen, wenn ein Mensch die Entscheidung nur „abnickt" und ohne inhaltliche Prüfung rein formal bestätigt.[674] Teilweise werden darüber hinaus aber nur sehr geringe Anforderungen gestellt und es für ausreichend erachtet, wenn sich die Möglichkeit zu einer abweichenden Entscheidung auf das „Herausfiltern von unplausiblen Entscheidungen" beschränkt.[675] Überzeugender erscheint es – jedenfalls im grundrechtssensiblen Bereich der Strafverfolgung –[676] zu fordern, dass eine echte inhaltliche Kontrolle von einer fachlich qualifizierten Person vorgenommen wird, die auch die rechtliche Kompetenz zu einer abweichenden Entscheidung hat.[677] Gerade bei einer fehleranfälligen Maßnahme wie der automatisierten Gesichtserkennung sollte daher eine im Abgleich von Gesichtern geschulte Person (z. B. eine Lichtbildsachverständige oder Lichtbildexpertin) eingesetzt werden, die zudem Funktionsweise, Fehlerrate und Verzerrungen von Gesichtserkennungssystemen zumindest in ihren Grundzügen versteht. Eine nur stichprobenartige Kontrolle genügt dabei nicht;[678] jeder Treffer muss überprüft werden.

672 So wohl auch, allerdings ohne nähere Begründung, *Radtke*, RDi 2024, 353, 357.
673 Vgl. außerdem zu Art. 22 DSGVO jüngst etwa *Paal/Hüger*, MMR 2024, 540.
674 Paal/Pauly/*Martini*, 3. Aufl. 2021, DSGVO Art. 22 Rn. 19; *Scholz*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, DSGVO Art. 22 Rn. 26; *Golla*, NJW 2021, 667, 672.
675 BeckOK DatenschutzR/*von Lewinski*, 46. Ed., Stand: 1.11.2023, DSGVO Art. 22 Rn. 25.1.
676 Mit Blick auf Art. 22 DGSVO (die „Schwestervorschrift" zu Art. 11 JI-RL) wurde vorgeschlagen, die Anforderungen an die menschliche Kontrolle einzelfallabhängig nach dem Anwendungskontext zu stellen, siehe *Steinbach*, Regulierung algorithmenbasierter Entscheidungen, 2021, 132 f.
677 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, 2023, 570 f. mwN.
678 Paal/Pauly/*Martini*, 3. Aufl. 2021, DSGVO Art. 22 Rn. 19.

Unabhängig davon, wie man Art. 26 Abs. 10 Uabs. 3 S. 2 KI-VO versteht: Es erscheint in jedem Fall sinnvoll – auch wenn die Vorschrift unmittelbar gilt (Art. 288 Abs. 2 AEUV) – diese Vorgaben direkt in einer Rechtsgrundlage zum Einsatz automatisierter Gesichtserkennung zu verankern. Dies gilt umso mehr, da die Vorschrift ohnehin nur speziell für die nachträgliche biometrische Fernidentifizierung gilt.

e) Fazit

Die KI-Verordnung enthält eine Reihe von Vorschriften für Hochrisiko-KI-Systeme, darunter für Gesichtserkennungssysteme. Diese Vorgaben können zumindest dazu beitragen, dass künftige Systeme keine oder weniger Verzerrungen in der Erkennungsgenauigkeit zulasten einzelner Bevölkerungsgruppen aufweisen. Da nicht konkret festgelegt wird, wie die Genauigkeit zu messen ist, darf die praktische Bedeutung dieser Vorschriften aber nicht überbewertet werden.

Nicht adressiert werden andere Gründe, die dazu führen können, dass bestimmte Bevölkerungsgruppen häufiger von Fehlidentifizierungen im Zusammenhang mit Gesichtserkennung betroffen sein könnten. Insbesondere die Frage, wie die Datenbank zusammengesetzt ist, die zum Abgleich verwendet wird, spielt hier eine entscheidende Rolle. Wenn mehr Personen einer bestimmten Ethnie erkennungsdienstlich behandelt werden und daher häufiger in polizeilichen Datenbanken auftauchen, dann steigt auch ihr Risiko, fehlerhaft identifiziert zu werden. Solche „sozialen Verzerrungen" blendet die KI-Verordnung aus, sie adressiert in diesem Zusammenhang nur statistische Verzerrungen durch nicht repräsentative Datensätze.

Individuelle Rechte werden den von den KI-Systemen betroffenen Menschen (bis auf Art. 86 KI-VO) nicht zugesprochen, insbesondere besteht keine Pflicht, sie von der Verwendung (z. B. automatisierter Gesichtserkennung) zu benachrichtigen.[679]

Es ist fraglich, ob die Vorgaben der KI-Verordnung geeignet sind, einen Automation bias,[680] also ein blindes Vertrauen auf die Vorschläge von KI-Systemen, zu verhindern. Die Vorschriften zur menschlichen Aufsicht regeln vorrangig *technische* Vorkehrungen. Ob dies ausreicht, ist zweifelhaft.

679 *Hoffmann*, Der nichtstaatliche Einsatz biometrischer Gesichtserkennungssysteme nach der DSGVO, 2023, 273 schlussfolgert daher zutreffend, dass die Autonomie der Betroffenen durch die KI-Verordnung nicht gestärkt wird.

680 Hierzu näher Kapitel III. B. II. 3.

Gerade im Kontext von Gesichtserkennung gibt es eine Reihe anderer als technischer Ursachen für ein leichtsinniges Verlassen auf die Ergebnisse einer Maschine, siehe hierzu Kapitel III. B. II. 2. Auch ist die Auslegung von Art. 26 Abs. 10 Uabs. 3 S. 2 KI-VO unklar, sodass hierdurch keine rechtssicheren und verbindlichen Vorgaben zur menschlichen Beteiligung geschaffen werden.

Insgesamt sollten die (spärlichen) Regelungen zu automatisierter Gesichtserkennung in der KI-Verordnung für die Mitgliedstaaten, darunter Deutschland, kein Grund sein, sich auszuruhen. Im Gegenteil, dieser äußerste Rahmen der KI-Verordnung sollte eine Aufforderung sein, nun auf nationaler Ebene tätig zu werden.

2. JI-Richtlinie

Beim Einsatz automatisierter Gesichtserkennung durch deutsche Strafverfolgungsbehörden sind zudem die Vorgaben der JI-Richtlinie[681] zu beachten.[682] Diese 2016 in Kraft getretene Richtlinie der EU enthält Bestimmungen 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, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit (Art. 1 Abs. 1 JI-RL). Hingegen ist die DSGVO auf diesem Gebiet ausdrücklich nicht anwendbar, vgl. Art. 2 Abs. 2 lit. d DSGVO.

Der Anwendungsbereich der JI-Richtlinie ist nach Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 JI-RL eröffnet, wenn personenbezogene Daten durch die zuständigen Behörden zur Strafverfolgung oder Gefahrenabwehr verarbeitet werden. Verarbeitung meint dabei „jeden mit oder ohne Hilfe automati-

681 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 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 und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119, 89, berichtigt durch 2018 L 127, 9 und 2021 L 74, 36). Zu Anwendbarkeit und Kompetenzmäßigkeit der JI-Richtlinie ausführlich *Schindler*, Biometrische Videoüberwachung, 2021, 240 ff.

682 Zur Anwendung der Regelungen der JI-Richtlinie auf Gesichtserkennung siehe auch *Europäischer Datenschutzausschuss*, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, Version 2.0, 2023, 19 ff.

sierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung" (Art. 3 Nr. 2 JI-RL). Die JI-Richtlinie gilt nach Art. 2 Abs. 2 JI-RL für die „ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen". Daher fällt letztendlich jeder Umgang mit personenbezogenen Daten zu Zwecken der Strafverfolgung oder Gefahrenabwehr in den Anwendungsbereich der Richtlinie.[683] Der Einsatz automatisierter Gesichtserkennung – bei dem personenbezogene (biometrische) Daten automatisiert verarbeitet werden – ist hiervon ohne Weiteres erfasst.[684]

Der Gesetzgeber hat sich gegen eine Umsetzung der Vorgaben der JI-Richtlinie im jeweiligen Fachgesetz (z. B. StPO) entschieden und stattdessen entsprechende Regelungen im BDSG getroffen. Wie *Rückert* allerdings ausführlich und überzeugend darlegt, ist die Umsetzung vielfach unzureichend.[685] Teilweise kann dies durch richtlinienkonforme Auslegung „korrigiert" werden.[686]

Die JI-Richtlinie enthält eine Reihe an Vorschriften, die auch für den Einsatz automatisierter Gesichtserkennung in der Strafverfolgung relevant sind. Allerdings gelten diese Vorgaben für alle von der Richtlinie erfassten Datenverarbeitungen; sie wären daher meist sinnvollerweise nicht in jeder einzelnen Rechtsgrundlage (darunter z. B. einer Rechtsgrundlage für automatisierte Gesichtserkennung), sondern in einer Art allgemeinem Teil (z. B. in der StPO oder – wie derzeit versucht – im BDSG) zu regeln.[687] Die nähere Ausgestaltung bedürfte einer eigenen ausführlichen Untersuchung.

683 Siehe auch *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, 2023, 516.

684 *Schindler*, Biometrische Videoüberwachung, 2021, 672 mwN.

685 Vertiefend zu den einzelnen Vorgaben der JI-Richtlinie und ihrer jeweiligen Umsetzung im BDSG *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, 2023, 524 ff.; vgl. auch *Schwichtenberg*, NK 2020, 91, 101 ff.

686 Siehe etwa *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, 2023, 546.

687 In einigen Fällen bieten sich aber Konkretisierungen direkt in der jeweiligen Rechtsgrundlage an, z. B. zur Ausgestaltung der Benachrichtigungspflicht (Art. 13 JI-RL) bei der jeweiligen Maßnahme.

In dieser Arbeit wird stattdessen auf drei Vorschriften der JI-Richtlinie eingegangen, die bei der automatisierten Gesichtserkennung besonders relevant werden: Art. 8 Abs. 2 JI-RL (Konkretisierung der Anforderungen an die Bestimmtheit und Normenklarheit), Art. 10 JI-RL (Verarbeitung besonderer Kategorien personenbezogener Daten) und Art. 11 JI-RL (automatisierte Entscheidungsfindung im Einzelfall).

a) Art. 8 Abs. 2 JI-RL

Wer – anders als hier vertreten[688] – nicht bereits aus verfassungsrechtlichen Gründen fordert, dass die Verarbeitung biometrischer Merkmale in einer Rechtsgrundlage zum Einsatz automatisierter Gesichtserkennung genannt wird, muss anerkennen, dass dieses Erfordernis jedenfalls aus Art. 8 Abs. 2 JI-RL folgt. Diese Vorschrift macht Vorgaben zur Ausgestaltung strafprozessualer Rechtsgrundlagen, die eine Datenverarbeitung erlauben. Nach Art. 8 Abs. 2 JI-RL müssen im „Recht der Mitgliedstaaten, das die Verarbeitung innerhalb des Anwendungsbereichs dieser Richtlinie regelt, […] zumindest die Ziele der Verarbeitung, die personenbezogenen Daten, die verarbeitet werden sollen, und die Zwecke der Verarbeitung angegeben" werden. Ausdrücklich schreibt Art. 8 Abs. 2 JI-RL also vor, dass „die personenbezogenen Daten, die verarbeitet werden sollen" anzugeben sind.[689] In einer Rechtsgrundlage, die den Einsatz automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger erlaubt, müsste also zum Ausdruck kommen, dass *biometrische* Daten verarbeitet werden.[690] Dies gilt umso mehr vor dem Hintergrund, dass – wie sogleich vertieft wird –

688 Kapitel II. A. I. 3. b); siehe auch Kapitel II. C. I. 2. d).

689 Hierzu auch *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, 2023, 533 f., der insofern wohl davon ausgeht, dass sich dieses Erfordernis nicht aus dem deutschen Verfassungsrecht ergibt („geht […] über die Anforderungen der verfassungsrechtlichen Normenklarheit und Bestimmtheit hinaus"). Anders wohl *Schindler*, Biometrische Videoüberwachung, 2021, 685, der davon ausgeht, dass sich durch Art. 8 Abs. 2 JI-RL keine gegenüber dem deutschen Verfassungsrecht erhöhten Anforderungen ergeben.

690 *Schindler*, Biometrische Videoüberwachung, 2021, 687 vertritt in diesem Zusammenhang, dass biometrische Daten nicht ausdrücklich als solche bezeichnet werden müssen, sondern dass es ausreiche, wenn in der Rechtsgrundlage der Vorgang (z. B. Abgleich von Videoaufnahmen mit einem Fahndungsbestand) beschrieben werde und „aus diesen Regelungen – gegebenenfalls in Verbindung mit der Gesetzesbegründung – hinreichend deutlich hervor[geht], dass der Einsatz biometrischer Verfahren zur Verarbeitung biometrischer Daten zulässig ist".

biometrische Daten zu den Daten besonderer Kategorien zählen, für die in Art. 10 JI-RL ein besonderes Schutzregime angeordnet wird.

b) Art. 10 JI-RL

Art. 10 JI-RL sieht erhöhte Vorgaben für die Verarbeitung besonderer Kategorien personenbezogener Daten vor, dazu zählen biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person. Diese Anforderungen müssen zusätzlich zu den Regelungen der KI-Verordnung zur biometrischen Fernidentifizierung gewahrt werden (ErwG 39 KI-VO). Die Verarbeitung besonderer Kategorien personenbezogener Daten ist nach Art. 10 JI-RL nur dann erlaubt, wenn sie „unbedingt erforderlich" ist und vorbehaltlich „geeigneter Garantien für die Rechte und Freiheiten der betroffenen Person" erfolgt. Außerdem muss sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zulässig sein (lit. a) *oder* der Wahrung lebenswichtiger Interessen der betroffenen oder einer anderen natürlichen Person dienen (lit. b) *oder* sich auf Daten beziehen, die die betroffene Person offensichtlich öffentlich gemacht hat (lit. c). Dabei sind die Einschränkungen des Art. 10 lit. b und lit. c im Rahmen des Strafprozessrechts nicht weiter von Bedeutung, da wegen des Gesetzesvorbehalts bei der Verarbeitung personenbezogener Daten ohnehin immer eine Rechtsgrundlage (lit. a) vorliegen muss.[691] Die entscheidenden Fragen sind daher, wann eine Datenverarbeitung „unbedingt erforderlich" ist und was „geeignete Garantien für die Rechte und Freiheiten der betroffenen Person" sind.

Mit Blick auf die Formulierung „unbedingt erforderlich" ist zunächst festzuhalten, dass sich eine solche zwar auch in Art. 26 Abs. 10 S. 2 KI-VO findet, der Regelungen zur nachträglichen Fernidentifizierung trifft. Allerdings bestehen feine Unterschiede in der Formulierung: Während Art. 10 JI-RL darauf abstellt, dass die *Verarbeitung der Daten* unbedingt erforderlich sein muss, wird in Art. 26 Abs. 10 S. 2 KI-VO formuliert, dass die Verwendung biometrischer Fernidentifizierung (also die Datenverarbeitung) auf das für die Ermittlung einer bestimmten Straftat unbedingt erforderliche *Maß* zu beschränken ist (vgl. auch ErwG 95 KI-VO: unbedingt erforderliche *Weise*). Art. 10 JI-RL adressiert mit der „unbedingten Erforderlichkeit" das „*Ob*" der Datenverarbeitung, Art. 26 Abs. 10 S. 2 KI-VO das „*Wie*".

691 So auch *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, 2023, 537.

Daher enthält Art. 10 JI-RL gegenüber der KI-Verordnung insofern eine zusätzliche Voraussetzung. Entscheidend ist deshalb, was genau damit gemeint ist, dass die Datenverarbeitung „unbedingt erforderlich" sein muss. Dies ist in der datenschutzrechtlichen Literatur umstritten;[692] so wird etwa vertreten, dass eine besonders strenge Verhältnismäßigkeitsprüfung erforderlich sei,[693] dass die Einschätzungsprärogative der verantwortlichen datenverarbeitenden Stelle eingeschränkt werde,[694] dass die Datenverarbeitung „beinahe unverzichtbar"[695] sein müsse oder dass eine „Vorgewichtung der Verhältnismäßigkeitsprüfung ieS zugunsten der grundrechtlichen Interessen des Betroffenen" stattfinde[696]. Einigkeit besteht aber zumindest dahingehend, dass die Anforderungen über eine normale Verhältnismäßigkeitsprüfung hinausgehen. Die „unbedingte Erforderlichkeit" der Verarbeitung biometrischer Merkmale stellt insofern eine zusätzliche Voraussetzung dar, die beim Einsatz automatisierter Gesichtserkennung zu beachten ist. Dies kann entweder dadurch erreicht werden, dass in einer Rechtsgrundlage für automatisierte Gesichtserkennung das Erfordernis der „unbedingten Erforderlichkeit" der Datenverarbeitung direkt verankert wird oder dadurch, dass neben der Rechtsgrundlage für automatisierte Gesichtserkennung immer auch die Vorschrift des § 48 BDSG zu beachten ist,[697] die deutsche Umsetzungsnorm[698] zu Art. 10 JI-RL. Ersteres erscheint vorzugswürdig, da durch eine Regelung direkt in der Rechtsgrundlage besser sichergestellt werden kann, dass die „unbedingte Erforderlichkeit" der Datenverarbeitung tatsächlich geprüft wird. Derzeit scheinen die Strafverfolgungsbehörden, soweit bekannt, nämlich beim Einsatz automatisierter Gesichtserkennung § 48 BDSG nicht heranzuziehen.[699]

Art. 10 JI-RL schreibt außerdem vor, dass die Verarbeitung besonderer Kategorien personenbezogener Daten „geeigneter Garantien für die Rechte und Freiheiten der betroffenen Person" bedarf. Diese Vorgabe hat der deut-

692 Siehe etwa den Überblick und die Nachweise bei *Arzt*, DÖV 2023, 991, 996.
693 BeckOK DatenschutzR/*Albers/Schimke*, 46. Ed., Stand: 1.8.2023, BDSG § 48 Rn. 28; wohl auch *Schindler*, Biometrische Videoüberwachung, 2021, 684 f.
694 Paal/Pauly/*Frenzel*, 3. Aufl. 2021, BDSG § 48 Rn. 3.
695 Kühling/Buchner/*Schwichtenberg*, 4. Aufl. 2024, BDSG § 48 Rn. 3.
696 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, 2023, 575 f.
697 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, 2023, 537; Kühling/Buchner/*Schwichtenberg*, 4. Aufl. 2024, BDSG § 48 Rn. 5; Gola/Heckmann/*Braun*, 3. Aufl. 2022, BDSG § 48 Rn. 11.
698 Vgl. BT-Drs. 18/11325, 111; kritisch zur Umsetzung des Art. 10 JI-RL durch § 48 BDSG *Arzt*, DÖV 2023, 991, 996 ff.
699 Siehe etwa BT-Drs. 19/14952, 2 f.

sche Gesetzgeber in § 48 Abs. 2 BDSG umgesetzt („Werden besondere Kategorien personenbezogener Daten verarbeitet, sind geeignete Garantien für die Rechtsgüter der betroffenen Personen vorzusehen.") und dabei einen nicht abgeschlossenen Katalog möglicher Schutzmaßnahmen benannt. Geeignete Garantien können, so § 48 Abs. 2 BDSG, insbesondere sein: spezifische Anforderungen an die Datensicherheit oder die Datenschutzkontrolle (Nr. 1), die Festlegung von besonderen Aussonderungsprüffristen (Nr. 2), die Sensibilisierung der an Verarbeitungsvorgängen Beteiligten (Nr. 3), die Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der verantwortlichen Stelle (Nr. 4), die von anderen Daten getrennte Verarbeitung (Nr. 5), die Pseudonymisierung personenbezogener Daten (Nr. 6), die Verschlüsselung personenbezogener Daten (Nr. 7) oder spezifische Verfahrensregelungen, die im Fall einer Übermittlung oder Verarbeitung für andere Zwecke die Rechtmäßigkeit der Verarbeitung sicherstellen (Nr. 8). Das Ergreifen dieser oder anderer Schutzmaßnahmen liegt damit im Ermessen der zuständigen Behörde.[700]

Diese Umsetzung dürfte den Anforderungen des verfassungsrechtlichen Gebots der Bestimmtheit und Normenklarheit nicht gerecht werden. Jedenfalls bei erheblichen Eingriffen – und das ist bei Verarbeitung der in Art. 10 JI-RL genannten Daten regelmäßig der Fall – müssten die Schutzmaßnahmen vom Gesetzgeber (und unter Umständen auch spezifisch für die jeweilige Datenverarbeitung) festgelegt werden.[701] Bei einer eingriffsintensiven Maßnahme wie der automatisierten Gesichtserkennung sollten diese Vorgaben vorrangig von der Legislative geschaffen werden. Welche Schutzmaßnahmen erforderlich und zweckmäßig sind, bedarf auch einer näheren Untersuchung der internen Vorgänge der Strafverfolgungsbehörden, die hier nicht geleistet werden kann. Weitere sinnvolle Garantien – wie sie auch in dieser Arbeit vorgeschlagen werden – wären etwa ein Richtervorbehalt, eine verpflichtende Überprüfung der Suchergebnisse durch Lichtbildsachverständige und -experten, Schulungen innerhalb der Polizei zum Umgang mit Gesichtserkennungstreffern und Berichte für die Öffentlichkeit.

700 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, 2023, 539; BeckOK DatenschutzR/*Albers/Schimke*, 46. Ed., Stand: 1.8.2023, BDSG § 48 Rn. 32; Gola/Heckmann/*Braun*, 3. Aufl. 2022, BDSG § 48 Rn. 14.

701 In diese Richtung wohl auch *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, 2023, 539; *Schantz/Wolff*, Das neue Datenschutzrecht, 2017, Rn. 722; Gola/Heckmann/*Braun*, 3. Aufl. 2022, BDSG § 48 Rn. 15. Anders *Schindler*, Biometrische Videoüberwachung, 2021, 689. Differenzierend BeckOK DatenschutzR/*Albers/Schimke*, 46. Ed., Stand: 1.8.2023, BDSG § 48 Rn. 32.

c) Art. 11 JI-RL

Zu untersuchen ist außerdem, ob Art. 11 JI-RL[702] gegenüber dem Verfassungsrecht und der KI-Verordnung zusätzliche Vorgaben für den Einsatz automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger macht. Art. 11 Abs. 1 JI-RL verbietet grundsätzlich automatisierte Entscheidungen, die eine nachteilige Rechtsfolge für die betroffene Person haben oder sie erheblich beeinträchtigen.[703] Eine Ausnahme besteht, wenn eine automatisierte Entscheidung nach dem Unionsrecht oder dem Recht des entsprechenden Mitgliedstaats erlaubt ist und dort geeignete Garantien für die Rechte und Freiheiten der betroffenen Person (zumindest aber das Recht auf persönliches Eingreifen seitens des Verantwortlichen) festgelegt sind. Art. 11 Abs. 2 JI-RL erhöht diese Anforderungen an Schutzgarantien noch einmal für Entscheidungen, die auf besonderen Kategorien personenbezogener Daten nach Art. 10 JI-RL beruhen; dazu gehört automatisierte Gesichtserkennung, da hier biometrische Daten verarbeitet werden.

aa) Verhältnis zu Art. 26 Abs. 10 Uabs. 3 S. 2 KI-VO

Fraglich ist zunächst das Verhältnis von Art. 11 Abs. 1, 2 JI-RL zu Art. 26 Abs. 10 Uabs. 3 S. 2 KI-VO.[704] Letzterer schreibt vor, dass die Strafverfolgungsbehörden keine ausschließlich auf der Grundlage der Ausgabe von

702 Die Vorschrift wurde im deutschen Recht in § 54 BDSG umgesetzt, allerdings nicht vollständig, siehe hierzu *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, 2023, 573 f.; Sydow/Marsch DS-GVO/BDSG/*Helfrich*, 3. Aufl. 2022, BDSG § 54 Rn. 5.

703 Zu einer Nähe des grundsätzlichen Verbots vollautomatisierter Entscheidungen (Art. 11 Abs. 1 JI-RL bzw. die „Schwestervorschrift" Art. 22 Abs. 1 DSGVO) zur Menschenwürde etwa *Paal/Hüger*, MMR 2024, 540; *Radtke*, RDi 2024, 353, 355 f.; *Malorny*, RdA 2022, 170, 176; *Malorny*, JuS 2022, 289, 295; *Golla*, NJW 2021, 667, 672; *Golla*, in: Chibanguza/Kuß/Steege, Künstliche Intelligenz, 2022, 2. Teil: § 9 A. KI-Einsatz bei der Polizei Rn. 12 f.; Paal/Pauly/*Martini*, 3. Aufl. 2021, DSGVO Art. 22 Rn. 29b; *Geminn*, DÖV 2020, 172, 176; *Golla*, DÖV 2019, 673, 678 f.; *Golla*, in: Donath/Bretthauer u. a., Verfassungen – ihre Rolle im Wandel der Zeit. 59. Assistententagung Öffentliches Recht, 2019, 183, 196; *Orwat*, Diskriminierungsrisiken durch Verwendung von Algorithmen, 2019, 91 f.; *Ernst*, JZ 2017, 1026, 1030; *Martini*, DÖV 2017, 443, 452; in eine ähnliche Richtung auch *Vasel/Heck*, NVwZ 2024, 540, 544.

704 Zum Unterschied zwischen Art. 11 JI-RL und Art. 14 Abs. 5 Uabs. 1 KI-VO gilt das oben (Kapitel II. B. I. 1. d) cc) zum Unterschied zwischen Art. 26 Abs. 10 Uabs. 3 S. 2 KI-VO und Art. 14 Abs. 5 Uabs. 1 KI-VO Gesagte.

Systemen zur nachträglichen biometrischen Fernidentifizierung beruhende Entscheidung treffen dürfen, aus der sich eine nachteilige Rechtsfolge für eine Person ergibt. Zwischen Art. 26 Abs. 10 Uabs. 3 S. 2 KI-VO einerseits und Art. 11 Abs. 1, 2 JI-RL andererseits bestehen mehrere Unterschiede:

Erstens bezieht sich Art. 26 Abs. 10 Uabs. 3 S. 2 KI-VO nur auf Systeme zur nachträglichen biometrischen Fernidentifizierung (in der Strafverfolgung), Art. 11 Abs. 1, 2 JI-RL hingegen allgemein auf Strafverfolgungsmaßnahmen.[705] Zweitens verbietet Art. 26 Abs. 10 Uabs. 3 S. 2 KI-VO nur eine automatisierte Entscheidung, aus der sich eine „nachteilige Rechtsfolge" für eine Person ergibt; Art. 11 Abs. 1, 2 KI-VO untersagt hingegen grundsätzlich eine automatisierte Entscheidung, die eine „nachteilige Rechtsfolge" für die betroffene Person hat *oder* sie *„erheblich beeinträchtigt"*. Zwischen einer nachteiligen Rechtsfolge und einer erheblichen Beeinträchtigung besteht jedoch ein Unterschied;[706] letztere ist weiter zu verstehen und umfasst etwa auch nur faktisch (nicht rechtlich) beeinträchtigende Maßnahmen wie Ermittlungsmaßnahmen bei Dritten, die für den Beschuldigten stigmatisierende Wirkung haben.[707] Drittens liegt ein beträchtlicher Unterschied zwischen Art. 26 Abs. 10 Uabs. 3 S. 2 KI-VO und Art. 11 Abs. 1, 2 JI-RL darin, dass ersterer die entsprechenden automatisierten Entscheidungen absolut verbietet, während letzterer Ausnahmen vorsieht (Rechtsgrundlage im Unions- oder entsprechenden mitgliedstaatlichen Recht und Schutzgarantien).

Die KI-Verordnung enthält an mehreren Stellen Aussagen zu ihrem Verhältnis zu Vorgaben der JI-Richtlinie (siehe etwa ErwG 38, 39, 70, 94, 95 KI-VO), nicht jedoch zu Art. 11 JI-RL. Wäre Art. 26 Abs. 10 Uabs. 3 S. 2 KI-VO eine lex specialis Regelung[708], die Art. 11 JI-RL verdrängt, würde dies insbesondere bedeuten, dass im Zusammenhang mit biometrischer Fernidentifizierung eine automatisierte Entscheidung, die „nur" eine *erhebliche Beeinträchtigung* (so Art. 11 Abs. 1 JI-RL) verursacht – statt einer

705 In beiden Fällen sind auch (nach deutschem Verständnis) gefahrenabwehrrechtliche Maßnahmen erfasst.

706 Siehe zu Art. 11 JI-RL *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, 2023, 569 f.

707 Überzeugend *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, 2023, 569.

708 *Eisenberger*, in: Martini/Wendehorst, KI-VO, Art. 26 Rn. 61 vertritt, dass aus der Regelung des Art. 26 Abs. 10 Uabs. 3 S. 2 KI-VO „im Umkehrschluss […] [folgt], dass Entscheidungen, die keine nachteiligen Rechtsfolgen nach sich ziehen, alleine auf Grundlage der Ausgabe eines nachträglichen biometrischen Fernidentifizierungssystems getroffen werden können". Allerdings bleibt unklar, ob sie damit tatsächlich auch eine Verdrängung von Art. 11 Abs. 1, 2 JI-RL meint.

nachteiligen Rechtsfolge – nicht verboten, sondern erlaubt ist. In dieser Hinsicht wäre dann das Schutzniveau des Art. 11 Abs. 1 JI-RL für den Bereich der nachträglichen biometrischen Fernidentifizierung abgesenkt. Dies kann wohl kaum gewollt sein, zumal die KI-Verordnung in den Erwägungsgründen den eingriffsintensiven Charakter der nachträglichen biometrischen Fernidentifizierung ausdrücklich betont[709] und gerade zu dieser speziellen Strafverfolgungsmaßnahme – anders als zu anderen Strafverfolgungsmaßnahmen – besondere Regelungen schafft (insbesondere Art. 26 Abs. 10 KI-VO). Es ist daher davon auszugehen, dass die Schutzvorkehrungen des Art. 26 Abs. 10 Uabs. 3 S. 2 KI-VO einerseits und des Art. 11 Abs. 1, 2 JI-RL anderseits nebeneinander bestehen.

Art. 26 Abs. 10 Uabs. 3 S. 2 KI-VO enthält insofern ein höheres Schutzniveau, dass *ohne Ausnahmemöglichkeit* die dort erwähnten automatisierten Entscheidungen verboten werden, aus denen sich eine nachteilige Rechtsfolge für eine Person ergibt. Art. 11 Abs. 1, 2 JI-RL beinhaltet dahingehend einen weiteren Schutz, dass grundsätzlich auch automatisierte Entscheidungen, die zu erheblichen Beeinträchtigungen einer Person führen, untersagt sind.

bb) Weitergehende Vorgaben

Wie genau dieser (in Teilen) weitere Schutz des Art. 11 Abs. 1, 2 JI-RL beim Einsatz automatisierter Gesichtserkennung aussieht, hängt davon ab, wie man die Vorschrift auslegt.

Zunächst stellt sich die Frage, wann eine „Entscheidung, die eine [Person] erheblich beeinträchtigt", vorliegt. Der Begriff der „Entscheidung" ist dabei weit zu verstehen.[710] Teilweise wird – unter Verweis auf die Gesetzesbegründung zu § 54 BDSG – vertreten, dass hierunter nur Handlungen mit Außenwirkung fallen.[711] An der entsprechenden Stelle der Gesetzesbegründung findet sich der folgende Passus: „Um eine […] ‚Entscheidung, die eine nachteilige Rechtsfolge für die betroffene Person hat', zu sein, muss es sich

709 ErwG 95.

710 Vgl. nur zuletzt im SCHUFA-Urteil des EuGH zu Art. 22 DSG-VO, EuGH, Urt. v. 7.12.2023, OQ/Land Hessen, C-634/21, Rn. 44 ff.; dazu instruktiv etwa *Radtke*, RDi 2024, 353.

711 BeckOK DatenschutzR/*Mundil*, 46. Ed., Stand: 1.8.2023, BDSG § 54 Rn. 3b; Gola/Heckmann/*Braun*, 3. Aufl. 2022, BDSG § 54 Rn. 8.

bei einer solchen Entscheidung um einen Rechtsakt mit Außenwirkung gegenüber der betroffenen Person – regelmäßig einen Verwaltungsakt – handeln. Interne Zwischenfestlegungen oder -auswertungen, die Ausfluss automatisierter Prozesse sind, fallen nicht hierunter."[712] Dabei überzeugt allerdings bereits der Verweis auf diese Gesetzesbegründung in diesem Zusammenhang wenig, denn diese nennt nur die „Entscheidung, die eine nachteilige Rechtsfolge" hat, nicht die – in Art. 11 JI-RL, § 54 BDSG ebenfalls genannte und hier relevante – „Entscheidung, die eine [Person] erheblich beeinträchtigt".

Aber auch inhaltlich wäre es wenig überzeugend, unter „erhebliche beeinträchtigende Entscheidungen" nur Maßnahmen mit Außenwirkung zu subsumieren, denn dann hätte das Merkmal „erhebliche Beeinträchtigung" neben „nachteiliger Rechtsfolge" keine eigenständige Bedeutung mehr. Jede Maßnahme mit Außenwirkung in Strafverfolgung und Gefahrenabwehr hat zugleich eine nachteilige Rechtsfolge für die betroffene Person, denn sie ist zumindest verpflichtet, die Maßnahme zu dulden.[713]

Rückert erläutert dies überzeugend im Zusammenhang mit der Bejahung eines Anfangsverdachts: „Die bloße Bejahung eines Tatverdachts hat noch keine unmittelbare Außenwirkung gegenüber dem Tatverdächtigen. Diese entsteht erst durch die Ergreifung von Ermittlungsmaßnahmen auf Grundlage des Tatverdachts. Wegen des Legalitätsprinzips (§ 160 Abs. 1 StPO) muss die Staatsanwaltschaft nach Bejahung des Tatverdachts durch eine ausschließlich automatisierte Entscheidung Ermittlungsmaßnahmen gegenüber dem Tatverdächtigen ergreifen, um den Sachverhalt zu erforschen. Würde sich der Schutz von Art. 11 RL, § 54 BDSG in einem solchen Fall auf die Anordnung der Ermittlungsmaßnahmen beschränken, würde das Schutzziel – die Verhinderung von allein durch Maschinen getroffene, nachteilige Entscheidungen – nicht erreicht, weil zwar über das „Wie" der Maßnahmen noch von Menschen entschieden würde, wegen § 160 Abs. 1 StPO aber nicht mehr über das „Ob"." Dem ist zuzustimmen. Die Bejahung eines Anfangsverdachts ist bereits eine erheblich beeinträchtigende Entscheidung im Sinne des Art. 11 Abs. 1, 2 JI-RL.[714]

712 BT-Drs. 18/11325, 112.

713 So richtig *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, 2023, 569.

714 *Golla*, in: Chibanguza/Kuß/Steege, Künstliche Intelligenz, 2022, 2. Teil: § 9 A. KI-Einsatz bei der Polizei Rn. 13. Noch etwas weiter *Golla*, NJW 2021, 667, 672 Fn. 53, der hier wohl sogar eine „nachteilige Rechtsfolge" annimmt („Die Annahme eines Tatverdachts und die darauf beruhende Einleitung eines Ermittlungsverfahren[s] dürfte jedenfalls als nachteilige Rechtsfolge anzusehen sein."). Wohl auch *Martini*,

Für die automatisierte Gesichtserkennung bedeutet dies Folgendes: Wenn – wie derzeit im Rahmen des GES praktiziert – das Gesichtserkennungssystem nur eine Vorschlagsliste präsentiert und die tatsächliche Auswahl des Verdächtigen durch Lichtbildsachverständige und Lichtbildexperten erfolgt, dann dürfte erst mit der Auswahl durch diese Menschen ein (individualisierter) Anfangsverdacht anzunehmen sein. Die Bejahung des Anfangsverdachts erfolgt dann durch einen Menschen. Es muss sich allerdings bei dem Menschen um eine ausreichend geschulte und mit der Funktionsweise des Gesichtserkennungssystems vertraute Person mit hinreichender Entscheidungskompetenz zur Verwerfung der Gesichtserkennungstreffer handeln[715] und dieser Mensch muss den Treffer sinnvoll inhaltlich prüfen. Bei der Verwendung des GES geht die menschliche Beteiligung aktuell noch darüber hinaus, denn die Lichtbildsachverständigen und -experten überprüfen nicht nur einen Treffer, sondern wählen selbst aktiv aus der Kandidatenliste den Verdächtigen aus. Da der Anfangsverdacht dann überhaupt erst durch die Menschen individualisiert wird, liegt keine automatisierte Entscheidung im Sinne des Art. 11 Abs. 1, 2 JI-RL, § 54 BDSG vor.[716]

NVwZ-Extra 1-2/2022, 1, 5: Gesichtserkennungssoftware „trifft immerhin aber auf der Grundlage des Abgleichs mit einer Datenbank automatisiert die Entscheidung darüber, ob eine Person auszusondern ist und sich deshalb polizeiliche Maßnahmen anschließen. Alleine diese Aussonderungsentscheidung kann in Ausnahmefällen bereits eine erhebliche beeinträchtigende Wirkung hervorrufen, die den Tatbestand des Art. 11 JI-RL aktiviert.". Sehr weit etwa auch *Schantz/Wolff*, Das neue Datenschutzrecht, 2017, Rn. 738. Anders wohl Rademacher, AöR 2017, 366, 387 (allerdings im Kontext von Alarmmeldungen beim Predictive Policing, also im Bereich der Gefahrenabwehr, und noch zu § 6a Abs. 1 BDSG a. F.). Nicht ganz eindeutig bei *Rademacher*, in: Zimmer, Regulierung für Algorithmen und Künstliche Intelligenz, 2021, 229, 248.

715 Sie dazu die Ausführungen zu Art. 26 Abs. 10 Uabs. 3 S. 2 KI-VO und die entsprechenden Nachweise in Kapitel II. B. I. 1. d) cc).

716 Ob sich aus dem SCHUFA-Urteil des EuGH (zu Art. 22 DSGVO) eine andere Bewertung ergibt, bedürfte näherer Untersuchung. Nach dieser Entscheidung ist bereits die Erstellung eines Score-Werts (Prognose/Wahrscheinlichkeitswert mit Blick auf ein zukünftiges Verhalten wie z. B. die Rückzahlung eines Kredits) eine Entscheidung im Sinne des Art. 22 DSGVO, wenn dieser Score-Wert an einen dritten Verantwortlichen übermittelt wird und jener Dritte diesen Wert seiner Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit der betroffenen Person „maßgeblich" zugrunde legt (EuGH, Urt. v. 7.12.2023, OQ/Land Hessen, C-634/21, Rn. 40 ff.). Nach dem EuGH besteht eine Vermutung für die Maßgeblichkeit des Score-Werts, wenn „im Fall eines von einem Verbraucher an eine Bank gerichteten Kreditantrags ein unzureichender

Anders könnte dies sein, wenn die Überprüfung und Auswahl durch Experten abgeschafft und stattdessen automatisch der Top-1-Treffer des Gesichtserkennungssystems an den Ermittler weitergeleitet würde. Hier kann es zu Fällen kommen, in denen der Ermittler nicht in der Lage ist, den Treffer sinnvoll zu überprüfen – entweder mangels spezifischer Kompetenz im Vergleich von Gesichtern oder vor allem, weil er die (aus Sicht der Technologie bestehende) Ähnlichkeit nicht nachvollziehen[717] und begründen kann. Gerade bei sehr verschwommenen Bildern oder bei Bedeckung eines Großteils des Gesichts (z. B. mit einer Atemschutzmaske) kann dies vorkommen.[718] In solchen Fällen würde der Anfangsverdacht nicht mehr von einem Menschen begründet, sondern der Ermittler müsste und würde einzig auf das Ergebnis des Gesichtserkennungssystems abstellen. Dies wäre eine grundsätzlich unzulässige automatisierte Entscheidung im Sinne des Art. 11 Abs. 1, 2 JI-RL, § 54 BDSG. (Wohlbemerkt ist es dabei irrelevant, ob die Gesichtserkennungstechnologie besonders zuverlässig oder sogar zuverlässiger als Menschen funktioniert. Art. 11 JI-RL statuiert ein – in dieser Pauschalität durchaus kritikwürdiges – „Primat der menschlichen Letztentscheidung“[719].) Nicht ausreichend ist es dabei auch, wenn am Training des Algorithmus ein Mensch beteiligt ist, denn dadurch nimmt er keinen Einfluss auf die Entscheidung im Einzelfall.[720] Das bedeutet, dass eine Umstellung der Prozesse auf eine automatische Weiterleitung des Top-1-Treffer des Gesichtserkennungssystems direkt an den Ermittler als

---

Wahrscheinlichkeitswert in nahezu allen Fällen dazu [führt], dass die Bank die Gewährung des beantragten Kredits ablehnt.“ (Rn. 48). Übertragen auf das Sicherheitsrecht stellt sich daher die Frage, ob auch von einer automatisierten Entscheidung im Sinne des Art. 11 JI-RL auszugehen ist, wenn ein Wahrscheinlichkeitswert (z. B. eines Gesichtserkennungssystems im Hinblick auf die Ähnlichkeit zweier Gesichter) oberhalb einer bestimmten Schwelle in nahezu allen Fallen dazu führt, dass (von den überprüfenden Menschen) ein Anfangsverdacht bejaht wird.

717 In diese Richtung auch *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, 2023, 572 f. zu sog. Blackbox-Tools.

718 Genau genommen würde sich dieses Problem allerdings auch stellen, wenn Lichtbildsachverständige oder -experten den Top-1-Treffer überprüfen würden und es sich um ein Bild handelt, bei dem selbst Experten die vom Gesichtserkennungssystem bejahte Ähnlichkeit aber nicht mehr nachvollziehen können.

719 Gola/Heckmann/*Schulz*, 3. Aufl. 2022, DS-GVO Art. 22 Rn. 2; siehe auch *Radtke*, RDi 2024, 353, 355.

720 In diese Richtung auch *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, 2023, 570; BeckOK DatenschutzR/*von Lewinski*, 46. Ed., Stand: 1.11.2023, DSGVO Art. 22 Rn. 23.2; Paal/Pauly/*Martini*, 3. Aufl. 2021, DSGVO Art. 22 Rn. 19b; *Kumkar/Roth-Isigkeit*, JZ 2020, 277, 279.

automatisierte Entscheidung im Sinne des Art. 11 Abs. 1, 2 JI-RL, § 54 BDSG (mindestens) auch die Anforderungen des Art. 11 Abs. 1, 2 JI-RL, § 54 BDSG erfüllen muss. Erforderlich ist dafür eine ausdrückliche[721] Ermächtigung zur vollautomatisierten Entscheidungsfindung im Unionsrecht oder im nationalen Recht und Schutzgarantien im Sinne der Vorschrift.

d) Fazit

Aus der JI-Richtlinie ergeben sich zusätzliche Vorgaben für den Einsatz automatisierter Gesichtserkennung in der Strafverfolgung. Jedenfalls aus Art. 8 Abs. 2 JI-RL (wenn nicht bereits aus dem verfassungsrechtlichen Gebot der Bestimmtheit und Normenklarheit) folgt, dass die Verarbeitung biometrischer Daten ausdrücklich in der Rechtsgrundlage anzugeben ist. Aus Art. 10 JI-RL folgt, dass die Verarbeitung biometrischer Daten „unbedingt erforderlich" sein muss und dass die dort genannten Schutzmechanismen etabliert werden müssen. Der Vorschrift des Art. 11 Abs. 1, 2 JI-RL ist zu entnehmen, dass ohne ausdrückliche Rechtsgrundlage und entsprechende Schutzgarantien die Gesichtserkennungstreffer nicht ohne (echte inhaltliche) menschliche Kontrolle automatisch als Anfangsverdacht gewertet werden dürfen.

3. Grundrechte-Charta

Höhere oder konkretere Anforderungen, als sie das deutsche Verfassungsrecht stellt, sind für den Einsatz automatisierter Gesichtserkennung in der Strafverfolgung aus der EU-Grundrechte-Charta nicht abzuleiten.[722] Unionsrechtlich nicht vollständig determiniertes innerstaatliches Recht prüft jedenfalls das Bundesverfassungsgericht primär am Maßstab der Grund-

721 Vgl. auch *Schindler*, Biometrische Videoüberwachung, 2021, 694 f.

722 Siehe aber zum Bedeutungsgewinn der EU-Grundrechte-Charta (und der Rechtsprechung des EuGH und auch des EGMR) durch die JI-Richtlinie und ihre Umsetzung in den §§ 45 ff. BDSG, § 500 StPO *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, 2023, 528 ff.; siehe auch *Safferling/Rückert*, NJW 2021, 287 und bereits *Bäcker*, in: Hill/Kugelmann/Martini, Perspektiven der digitalen Lebenswelt, 2017, 63, 84 ff.

rechte des Grundgesetzes.[723] Der Einsatz von Gesichtserkennung in der Strafverfolgung richtet sich nach Vorschriften der Strafprozessordnung und nicht nach vollständig unionsrechtlich determiniertem Recht. Die JI-RL belässt den Mitgliedstaaten einen erheblichen Spielraum und setzt nur Mindeststandards;[724] Art. 1 Abs. 3 JI-RL sieht ausdrücklich vor, dass die Mitgliedstaaten strengere Vorgaben machen können. Auch die KI-Verordnung determiniert das innerstaatliche Recht mit Blick auf Gesichtserkennung nicht vollständig, denn sie enthält keine Rechtsgrundlage oder detaillierte Vorgaben für die Ausgestaltung einer solchen. Handelt es sich um unionsrechtlich nicht vollständig determiniertes Recht, dann stellt das nationale Verfassungsrecht den Prüfungsmaßstab des Bundesverfassungsgerichts.[725]

Daneben beanspruchen auch die Unionsgrundrechte Geltung, wenn die maßgeblichen Vorschriften (hier: der Strafprozessordnung) zugleich als Durchführung des Unionsrechts im Sinne des Art. 51 Abs. 1 S. 1 GRCh angesehen werden können.[726] Dabei können innerstaatliche Regelungen auch dann als Durchführung des Unionsrechts zu beurteilen sein, wenn für deren Gestaltung den Mitgliedstaaten Spielräume verbleiben, das Unionsrecht dieser Gestaltung aber einen „hinreichend gehaltvollen Rahmen setzt", der erkennbar auch unter Beachtung der Unionsgrundrechte konkretisiert werden soll.[727] Bejaht man beim Einsatz von Gesichtserkennung in der Strafverfolgung eine Anwendbarkeit der Unionsgrundrechte,[728] dann wären insbesondere Art. 8 GRCh (Recht auf Schutz personenbezogener Daten) und Art. 7 GRCh (Recht auf Achtung des Privatlebens) heranzuziehen.[729]

723 Grundlegend BVerfGE 152, 152 LS 1; hierzu vertiefend etwa *Marsch*, ZEuS 2020, 597 und *Wendel*, JZ 2020, 157; siehe auch *Classen*, EuR 2022, 279.

724 Hierzu nur *Roggenkamp*, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, § 21 Datenschutz und präventive Tätigkeit der Polizei, 2019, Rn. 4. Siehe auch *Martini*, NVwZ-Extra 1-2/2022, 1, 5.

725 Grundlegend BVerfGE 152, 152 LS 1; siehe auch BVerfGE 155, 119 (163 ff.). Zu dem Ergebnis, dass mit Blick auf den Einsatz automatisierter Gesichtserkennung primär die Grundrechte des deutschen Verfassungsrechts maßgeblich sind, kommt auch *Martini*, NVwZ-Extra 1-2/2022, 1, 5.

726 Hierzu etwa BVerfGE 152, 152 (168). Vgl. auch EuGH, Urt. v. 21.12.2016, Tele2 Sverige und Watson u. a., C-203/15 u. a., EU:C:2016:970, Rn. 78 ff.; EuGH, Urt. v. 2.10.2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, Rn. 29 ff.

727 BVerfGE 152, 152 (170).

728 Vgl. *Schindler*, Biometrische Videoüberwachung, 2021, 262.

729 Der EuGH zieht beide Grundrechte gemeinsam heran, siehe nur EuGH, Urt. v. 21.12.2016, Tele2 Sverige und Watson u. a., C-203/15 u. a., EU:C:2016:970, Rn. 78 ff. Für einen Vorrang des Art. 8 GRCh bei Überschneidung mit Art. 7 GRCh hingegen etwa *Jarass*, GrCh, 4. Aufl. 2021, EU-Grundrechte-Charta Art. 8 Rn. 4.

Deren Vorgaben im Hinblick auf den Schutz vor staatlichen Maßnahmen im Sicherheitsrecht sind aber bislang nicht näher ausgeformt[730] und entsprechen ansonsten weitgehend den Anforderungen des Grundgesetzes.[731]

II. EMRK

Schließlich ist noch zu untersuchen, ob die EMRK[732] – ggf. in ihrer Auslegung durch den Europäischen Gerichtshof für Menschenrechte (EGMR) – höhere Voraussetzungen an den Einsatz von Gesichtserkennung zur Identifizierung unbekannter Verdächtiger stellt als das deutsche Verfassungsrecht. Die EMRK und die Rechtsprechung des EGMR dienen auf der Ebene des Verfassungsrechts als Auslegungshilfen für die Bestimmung von Inhalt und Reichweite von Grundrechten und rechtsstaatlichen Grundsätzen des Grundgesetzes.[733] Die nationalen Grundrechte sind daher grundsätzlich EMRK-konform auszulegen.[734] Mit Blick auf die beim Einsatz von Gesichtserkennung in der Strafverfolgung vor allem relevante Vorschrift des Art. 8 EMRK (Recht auf Achtung des Privat- und Familienlebens) gilt allerdings grundsätzlich dasselbe wie bei den Grundrechten der EU-Grundrechte-Charta: Sie enthält keine konkreten oder weitergehenden Vorgaben

730 *Eifert*, in: Herdegen/Masing/Poscher/Gärditz, Handbuch des Verfassungsrechts, 2021, § 18 Persönliche Freiheit, Rn. 133.

731 So allgemein mit Blick auf Art. 7 und 8 GRCh *Eifert*, in: Herdegen/Masing/Poscher/Gärditz, Handbuch des Verfassungsrechts, 2021, § 18 Persönliche Freiheit, Rn. 135. Zu dem Ergebnis, dass sich die Vorgaben der deutschen Grundrechte und der Unionsgrundrechte speziell mit Blick auf den Einsatz von Gesichtserkennung in der Strafverfolgung nicht wesentlich unterscheiden kommt auch *Schindler*, Biometrische Videoüberwachung, 2021, 386, 555 f. Siehe auch zum Eingriff durch Gesichtserkennung und zur Rechtfertigung *Europäischer Datenschutzausschuss*, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, Version 2.0, 2023, 14 ff.

732 Konvention zum Schutze der Menschenrechte und Grundfreiheiten v. 4.11.1950, SEV Nr. 005; durch das Gesetz über die Konvention zum Schutze der Menschenrechte und Grundfreiheiten v. 7.8.1952 (BGBl. 1952 II, 685) in Deutschland ratifiziert.

733 BVerfGE 111, 307 (317); stRspr.

734 Anders kann dies etwa bei einem mehrpoligen Grundrechtsverhältnis sein, in dem sich zwei Grundrechtsträger gegenüberstehen und daher ggf. das „Mehr" an Freiheit für den einen Grundrechtsträger zugleich ein „Weniger" für einen anderen bedeutet; siehe hierzu nur BVerfGE 128, 326 (371); vgl. auch *Wahl/Masing*, JZ 1990, 553. Dies ist beim Einsatz automatisierter Gesichtserkennung in der Strafverfolgung nicht der Fall.

als das Grundgesetz.[735] Im Jahr 2023 entschied der EGMR jedoch den ersten Fall über den staatlichen Einsatz von Gesichtserkennung in der Strafverfolgung.[736] Im Folgenden wird daher untersucht, welche Vorgaben für den Einsatz von Gesichtserkennung in Deutschland aus dieser Entscheidung abgeleitet werden können.

1. Glukhin v. Russland

Der Fall wurde oben bereits angesprochen[737] und basiert auf folgendem Sachverhalt: Der Beschwerdeführer Nikolay Sergeyevich Glukhin war mit der Moskauer U-Bahn gefahren und trug dabei eine lebensgroße Pappfigur des inhaftierten Kreml-Kritikers Konstantin Kotov mit sich, der ein Schild in Händen hatte mit der Aufschrift „А вы не о*уели? Я Константин Котов, за мирные пикеты мне грозит до 5 лет." („Seid ihr bescheuert? Ich bin Konstantin Kotov, mir drohen bis zu 5 Jahre wegen friedlichen Protests.").[738] Von der Protestaktion wurden Fotos und ein Video in den sozialen Medien hochgeladen; diese fand die Polizei und identifizierte den Demonstranten mit nachträglicher Gesichtserkennung.[739] Wenige Tage später wurde er in der U-Bahn festgenommen, offenbar lokalisiert durch Echtzeit-Gesichtserkennung.[740] Daraufhin wurde er zu einer Geldstrafe von etwa 283 Euro verurteilt, weil er seinen Protest nicht angemeldet hatte. Dies stellt nach russischem Recht eine Ordnungswidrigkeit dar (Art. 20.2 § 5 des russischen Ordnungswidrigkeitengesetzes). Dass die Polizei Gesichtserkennung eingesetzt hatte, gaben die Regierungsvertreter Russlands zwar während des Verfahrens vor dem EGMR nicht ausdrücklich zu. Die Richterinnen und Richter sahen die Verwendung aber als erwiesen an, weil nicht

735 *Schindler*, Biometrische Videoüberwachung, 2021, 357 f., 363 ff., 386, 396 ff.

736 EGMR, Urt. v. 4.7.2023, 11519/20. Wie bereits angesprochen, ist Russland zwar seit 16.9.2022 nicht mehr Vertragspartei der EMRK, für die Bearbeitung der bis zu diesem Zeitpunkt eingereichten Beschwerden gegen Russland ist der EGMR aber weiterhin zuständig, vgl. Art. 58 II EMRK.

737 Kapitel I. G. II. 1. b).

738 Hierzu die russische Nichtregierungsorganisation OVD-Info, 4.7.2023, https://perma.cc/LTU2-X85U; in der Entscheidung des EGMR findet sich die Formulierung „You must be f**king kidding me. I'm Konstantin Kotov. I'm facing up to five years [in prison] under [Article] 212.1 for peaceful protests.", EGMR, Urt. v. 4.7.2023, 11519/20 Rn. 7.

739 EGMR, Urt. v. 4.7.2023, 11519/20 Rn. 9 ff.

740 EGMR, Urt. v. 4.7.2023, 11519/20 Rn. 12.

erklärbar war, wie die Polizei den Demonstranten so schnell nach seinem Protest identifizieren konnte.[741] Da die russische Polizei den Einsatz von Gesichtserkennung nicht dokumentieren und Betroffene daher auch nicht darüber informiert werden müsse, sei es im Übrigen für die Bürger kaum möglich, den Einsatz zu beweisen.[742] Zudem gebe es zahlreiche weitere Fälle, in denen Demonstranten in Russland mit Gesichtserkennung identifiziert wurden.[743]

Der EGMR sieht in dem Einsatz von Gesichtserkennung zur Identifizierung und Lokalisierung von Glukhin einen Verstoß gegen Art. 8 Abs. 1 EMRK.[744] Einen Eingriff in Art. 8 Abs. 1 EMRK bejaht der EGMR sowohl mit Blick auf die nachträgliche als auch die Echtzeit-Gesichtserkennung.[745] Allerdings unterscheidet der Gerichtshof nicht näher zwischen den verschiedenen Schritten bei der Gesichtserkennung (Erstellung der Embeddings, Abgleich, Treffer).[746] Gem. Art. 8 Abs. 2 EMRK ist ein Eingriff gerechtfertigt, wenn er auf einer rechtlichen Grundlage beruht[747] und in einer demokratischen Gesellschaft notwendig ist für die nationale oder

741 EGMR, Urt. v. 4.7.2023, 11519/20 Rn. 72.

742 EGMR, Urt. v. 4.7.2023, 11519/20 Rn. 72.

743 EGMR, Urt. v. 4.7.2023, 11519/20 Rn. 70 und 40 unter Verweis auf die Berichte der russischen Nichtregierungsorganisation OVD-Info.

744 EGMR, Urt. v. 4.7.2023, 11519/20 Rn. 91. Zudem wurde ein Verstoß gegen Art. 10 EMRK wegen des Ordnungswidrigkeitenverfahrens festgestellt (Rn. 49 ff.).

745 EGMR, Urt. v. 4.7.2023, 11519/20 Rn. 69.

746 In EGMR, Urt. v. 4.7.2023, 11519/20 Rn. 68 beschreibt der Gerichtshof den Sachverhalt folgendermaßen: „In the present case, during routine monitoring of the Internet the police discovered photographs and a video of the applicant holding a solo demonstration published on a public Telegram channel. They made screenshots of the Telegram channel, stored them and allegedly applied facial recognition technology to them to identify the applicant. Having identified the location on the video as one of the stations of the Moscow underground, the police also collected video-recordings from CCTV surveillance cameras installed at that station as well as at two other stations through which the applicant had transited. They made screenshots of those video-recordings and stored them. They also allegedly used the live facial recognition CCTV cameras installed in the Moscow underground to locate and arrest the applicant several days later with the aim of charging him with an administrative offence. The screenshots of the Telegram channel and of the video-recordings from the CCTV surveillance cameras were subsequently used in evidence in the administrative-offence proceedings against the applicant." Im nächsten Abschnitt ist nur die Rede davon, dass die russische Regierung nicht widersprochen hat, dass diese tatsächlichen Umstände („the factual circumstances as described above") einen Eingriff in Art. 8 Abs. 1 EMRK begründen.

747 Dies muss kein formelles Gesetz sein, auch Richter- oder Gewohnheitsrecht kommt als Grundlage in Betracht; vgl. EGMR, Urt. v. 26.4.1979, 6538/74 Rn. 47 zu Art. 10.

öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer.[748] Dabei weist der EGMR auf seine bisherige Rechtsprechung hin, wonach im Zusammenhang mit dem Sammeln und Verarbeiten persönlicher Daten klare und detaillierte Vorschriften unverzichtbar sind, die Umfang und Anwendung solcher Maßnahmen regeln und Mindestanforderungen aufstellen, u. a. für die Dauer, Aufbewahrung und Verwendung, den Zugang Dritter, das Verfahren zur Sicherung der Integrität und Vertraulichkeit der Daten sowie ihre Vernichtung, also ausreichende Sicherungen gegen die Gefahr von Missbrauch und Willkür.[749] Im Zusammenhang mit dem Einsatz von Gesichtserkennungstechnologie betont der Gerichtshof nun, dass es erforderlich sei, den Anwendungsbereich und den Einsatz der Maßnahmen detailliert zu regeln („detailed rules governing the scope and application of measures") und strenge Schutzmaßnahmen gegen die Gefahr von Missbrauch und Willkür zu ergreifen.[750]

Mit Blick auf das russische Recht hält der EGMR fest, dass die Rechtsgrundlagen diesen Anforderungen nicht genügen. Insbesondere genüge auch die herangezogene Vorschrift des russischen Gesetzes zum Schutz persönlicher Daten nicht, die vorsieht, dass persönliche Daten im Zusammenhang mit der Beteiligung einer Person an irgendeinem gerichtlichen Verfahren („any judicial proceeding") verarbeitet werden können, und auch dann, wenn persönliche Daten von der betroffenen Person öffentlich zugänglich gemacht wurden.[751] Dieses Gesetz sei zu weit formuliert und auch nicht durch die russischen Gerichte restriktiv ausgelegt worden.[752] Das innerstaatliche Recht sehe keine Beschränkungen vor mit Blick auf die Art der Situationen, die zum Einsatz der Gesichtserkennungstechnologie führen können, die beabsichtigten Zwecke, die Kategorien von Personen, die ins Visier genommen werden können („targeted"), oder die Verarbeitung

748 Ausführlich zur Rechtfertigung von Eingriffen in Art. 8 Abs. 1 EMRK *Pätzold*, in: Karpenstein/Mayer, 3. Aufl. 2022, EMRK Art. 8 Rn. 90 ff.

749 EGMR, Urt. v. 4.7.2023, 11519/20 Rn. 91; siehe auch EGMR, Urt. v. 4.12.2008, 30562/04 u. 30566/04, Rn. 99.

750 EGMR, Urt. v. 4.7.2023, 11519/20 Rn. 82. Die Notwendigkeit von Schutzmaßnahmen sei umso größer, wenn es um den Einsatz der Technologie zur Live-Gesichtserkennung gehe.

751 EGMR, Urt. v. 4.7.2023, 11519/20 Rn. 83, 30.

752 EGMR, Urt. v. 4.7.2023, 11519/20 Rn. 83.

sensibler personenbezogener Daten.[753] Auch bestünden keine prozeduralen Sicherungsmechanismen beim Einsatz von Gesichtserkennungstechnologie in Russland, wie etwa Genehmigungsverfahren[754], Verfahren zur Prüfung, Verwendung und Speicherung der gewonnenen Daten, Kontrollmechanismen oder Rechtsbehelfe („remedies").[755]

Dann prüft der Gerichtshof die Verhältnismäßigkeit der Maßnahmen und stuft (auch) die nachträgliche Gesichtserkennung als besonders eingriffsintensiv ein („particularly intrusive").[756] Allerdings begründet er dies nicht näher, sondern verweist auf Auszüge der Richtlinien zu Gesichtserkennung (2021) des Beratenden Ausschusses des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten.[757] Es sei ein hohes Maß an Rechtfertigung („high level of justification") erforderlich, um den Einsatz als notwendig in einer demokratischen Gesellschaft anzusehen.[758] Zudem sei zu beachten, dass die verarbeiteten personenbezogenen Daten Informationen über die Teilnahme des Beschwerdeführers an einer friedlichen Demonstration enthielten und daher seine politische Meinung zum Gegenstand hatten.[759] Es handele sich daher um besonders sensible Daten, die ein erhöhtes Schutzniveau erforderten.[760] Bei der Beurteilung der „Notwendigkeit in einer demokratischen Gesellschaft" der Verarbeitung personenbezogener Daten im Rahmen von Ermittlungen sei die Art und Schwere der betreffenden Straftaten eines der zu berücksichtigenden Elemente.[761] Das innerstaatliche Recht in Russland erlaube aber die Verarbeitung biometrischer personenbezogener Daten im

753 EGMR, Urt. v. 4.7.2023, 11519/20 Rn. 83.
754 Vgl. EGMR, Urt. v. 4.7.2023, 11519/20 Rn. 83 („authorisation procedures").
755 EGMR, Urt. v. 4.7.2023, 11519/20 Rn. 83.
756 EGMR, Urt. v. 4.7.2023, 11519/20 Rn. 86.
757 EGMR, Urt. v. 4.7.2023, 11519/20 Rn. 86 mit Verweis auf Fn. 37 auf die Guidelines on Facial Recognition (2021) by the Consultative Committee of the Convention for the protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108), die mit Blick auf die Risiken allerdings auch nicht sehr spezifisch sind („Integrating facial recognition technologies into existing surveillance systems poses a serious risk to the rights to privacy and protection of personal data, as well as to other fundamental rights, since use of these technologies does not always require the awareness or co-operation of the individuals whose biometric data are processed in this way.").
758 EGMR, Urt. v. 4.7.2023, 11519/20 Rn. 86.
759 EGMR, Urt. v. 4.7.2023, 11519/20 Rn. 86.
760 EGMR, Urt. v. 4.7.2023, 11519/20 Rn. 86.
761 EGMR, Urt. v. 4.7.2023, 11519/20 Rn. 87.

Zusammenhang mit den Ermittlungen und der Verfolgung jeder Tat („offence"), unabhängig von deren Art und Schwere.[762]

Mit Blick auf den Beschwerdeführer stellt der Gerichtshof fest, dass er wegen einer geringfügigen Tat verfolgt wurde, die darin bestand, dass er ohne vorherige Anmeldung eine Einzeldemonstration abhielt – eine Tat, die nach innerstaatlichem Recht als Ordnungswidrigkeit und nicht als Straftat eingestuft wird („administrative rather than criminal").[763] Ihm sei nie vorgeworfen worden, während seiner Demonstration verwerfliche Handlungen wie Verkehrsbehinderung, Sachbeschädigung oder Gewalttaten begangen zu haben.[764] Auch sei nie behauptet worden, dass seine Aktionen eine Gefahr für die öffentliche Ordnung oder die Verkehrssicherheit dargestellt hätten.[765] Der EGMR hält zudem fest, dass der Einsatz von Gesichtserkennungstechnologien, die in hohem Maße in die Privatsphäre eingreifen, um Teilnehmer an friedlichen Protestaktionen zu identifizieren und festzunehmen, eine abschreckende Wirkung („chilling effect") auf das Recht auf Meinungs- und Versammlungsfreiheit haben könnte.[766] Unter diesen Umständen habe der Einsatz der Gesichtserkennungstechnologie zur Identifizierung des Beschwerdeführers anhand der Fotos und Videos sowie der Einsatz der Live-Gesichtserkennungstechnologie zur Lokalisierung und Verhaftung des Beschwerdeführers während seiner Fahrt mit der Moskauer U-Bahn nicht einem „dringenden sozialen Bedürfnis" entsprochen.[767]

Der EGMR kommt daher zu dem Schluss, dass der Einsatz einer stark in die Privatsphäre eingreifenden Gesichtserkennungstechnologie im Zusammenhang mit der Ausübung des Konventionsrechts des Beschwerdeführers auf freie Meinungsäußerung mit den Idealen und Werten einer demokratischen und rechtsstaatlichen Gesellschaft, die durch die Konvention erhalten und gefördert werden sollen, unvereinbar ist. Die Verarbeitung der personenbezogenen Daten des Beschwerdeführers mithilfe der Gesichtserkennungstechnologie im Rahmen eines Ordnungswidrigkeitenverfahrens – sowohl zur nachträglichen als auch zur Echtzeit-Gesichtserkennung – kön-

762 EGMR, Urt. v. 4.7.2023, 11519/20 Rn. 87.
763 EGMR, Urt. v. 4.7.2023, 11519/20 Rn. 88.
764 EGMR, Urt. v. 4.7.2023, 11519/20 Rn. 88.
765 EGMR, Urt. v. 4.7.2023, 11519/20 Rn. 88.
766 EGMR, Urt. v. 4.7.2023, 11519/20 Rn. 88.
767 EGMR, Urt. v. 4.7.2023, 11519/20 Rn. 89.

ne nicht als „notwendig in einer demokratischen Gesellschaft" angesehen werden.[768] Art. 8 EMRK sei daher verletzt worden.[769]

2. Schlussfolgerungen

Es handelt sich um die erste Entscheidung des EGMR zu Gesichtserkennung. Sie betrifft zwar direkt einen Fall der nachträglichen Gesichtserkennung zur Identifizierung eines unbekannten Verdächtigen, ihr können jedoch kaum hilfreiche Aussagen dahingehend entnommen werden, wie eine entsprechende Rechtsgrundlage ausgestaltet sein muss. Dem Urteil ist zunächst nur zu entnehmen, dass jedenfalls der Einsatz von Gesichtserkennung zur Verfolgung einer Ordnungswidrigkeit im Kontext einer friedlichen Versammlung und auf Grundlage einer allgemein gehaltenen Rechtsgrundlage nicht zulässig ist.

Beachtenswert ist jedoch, dass der Gerichtshof (auch) mit Blick auf die nachträgliche Gesichtserkennung von einer hohen Eingriffsintensität („particularly intrusive") ausgeht. Dies entspricht der in dieser Arbeit vertretenen Auffassung, dass es sich (nach deutschem Recht) um einen erheblichen Eingriff handelt. Allerdings ist unklar, womit der EGMR das hohe Eingriffsgewicht begründet. Auf die Streubreite – die anderen Personen, deren Gesichter abgeglichen werden – stellt er jedenfalls nicht ausdrücklich ab. Die Entscheidung ist aber ein deutlicher Fingerzeig an die Vertragsstaaten der EMRK: Die Verwendung von Gesichtserkennung erfordert ein hohes Maß an Rechtfertigung („high level of justification") und wirksame Schutzvorkehrungen.[770] Ob die in der KI-Verordnung auf EU-Ebene geregelten Fälle des zulässigen Einsatzes von Gesichtserkennung in der Strafverfolgung aus Sicht des EGMR ein solches Maß an Rechtfertigung erfüllen, bleibt abzuwarten.[771]

Hervorzuheben sind auch die Anforderungen, die der EGMR an eine Rechtsgrundlage stellt, nämlich dass der Anwendungsbereich und die Anwendung der Maßnahmen genau zu regeln sind. Diese Bestimmtheitserfordernisse werden sogleich bei der Untersuchung möglicher bereits im deutschen Strafprozessrecht existierender Rechtsgrundlagen relevant.

768 EGMR, Urt. v. 4.7.2023, 11519/20 Rn. 90.
769 EGMR, Urt. v. 4.7.2023, 11519/20 Rn. 91.
770 *Palmiotto/Menéndez González*, Computer Law & Security Review 2023, 105857, 1, 4.
771 Vgl. auch *Palmiotto/Menéndez González*, Computer Law & Security Review 2023, 105857, 1, 4.

Bemerkenswert ist zudem, dass der Gerichtshof den Versammlungskontext auch und gerade bei der Frage nach der Zulässigkeit der Gesichtserkennungsmaßnahmen hervorhebt. Wie oben erläutert,[772] sollte darüber nachgedacht werden, die Versammlungsfreiheit nicht nur bei der Frage zu berücksichtigen, wie tief der (ursprüngliche) Eingriff durch Videoüberwachung ist, sondern zudem direkt bei der Frage, ob und zur Verfolgung welcher Taten Gesichtserkennung eingesetzt werden darf, um Verdächtige nachträglich zu identifizieren. Aber auch der EGMR geht nicht von einem Eingriff in Art. 11 Abs. 1 EMRK (Versammlungs- und Vereinigungsfreiheit) aus, sondern belässt es bei einer Berücksichtigung im Rahmen der Verhältnismäßigkeitsprüfung des Art. 8 Abs. 1 EMRK.

Zu begrüßen ist auch, dass der EGMR ausdrücklich problematisiert, dass die Gesichtserkennung ohne Kenntnis des Betroffenen und auch ohne spätere Benachrichtigung eingesetzt wurde.[773] Er gewährt daher eine Beweiserleichterung; die Verwendung von Gesichtserkennung musste der Beschwerdeführer nicht näher nachweisen, da es keine andere plausible Erklärung dafür gab, wie die Polizei ihn so schnell finden konnte. Mit Blick auf eine Regulierung des Einsatzes von Gesichtserkennung im deutschen Recht sollte dies erneut eine Aufforderung sein, eine Benachrichtigungspflicht zu normieren.

III. Fazit

Die JI-Richtlinie, die EU-Grundrechte-Charta und die Rechtsprechung des EGMR zum Einsatz von Gesichtserkennung im Fall Glukhin v. Russland bekräftigen die Ergebnisse, die bereits mit Blick auf das deutsche Verfassungsrecht herausgearbeitet wurden. Insbesondere wird erneut deutlich, dass eine Ermächtigung zur Verwendung automatisierter Gesichtserkennung in besonderem Maße den Grundsätzen der Bestimmtheit und Verhältnismäßigkeit genügen muss. Der EGMR betont, dass der Anwendungsbereich und der Einsatz der Gesichtserkennung „detailliert" zu regeln und Schutzvorkehrungen vorzusehen seien. Die in dieser Arbeit vertretene Position, dass (auch) der Einsatz nachträglicher Gesichtserkennung

772 Kapitel II. A. II. 1. b).

773 Hierzu auch *Palmiotto/Menéndez González*, Computer Law & Security Review 2023, 105857, 1, 3 f.; vgl. zum Ganzen auch *Selinger/Hartzog*, Loyola Law Review 2019, 101; *Raposo*, European Journal on Criminal Policy and Research 2022, 515, 525 f.

zur Identifizierung unbekannter Verdächtiger ein im Sinne des deutschen Verfassungsrechts *erheblicher* Eingriff ist, wird vom EGMR im Hinblick auf die EMRK bekräftigt. Die JI-Richtlinie enthält einige zusätzliche Vorgaben im Hinblick auf die Bestimmtheit der Rechtsgrundlage (ausdrückliche Nennung biometrischer Daten), die „unbedingte Erforderlichkeit" und Schutzgarantien bei der Verarbeitung biometrischer Daten sowie Grenzen für vollautomatisierte Entscheidungen. Die KI-Verordnung enthält ebenfalls einige weitere Vorschriften für den Einsatz automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger. Nachträgliche Fernidentifizierungssysteme werden als Hochrisiko-KI eingeordnet und unterliegen daher den strengen Vorgaben für solche Systeme. Die Pflichten richten sich allerdings vorrangig an die Anbieter der Systeme, nicht an die Betreiber. Auch die Vorschrift, dass zwei natürliche Personen ein Identifizierungsergebnis bestätigen müssen, bevor weitere Maßnahmen getroffen werden, ist als Vorgabe an das Design des Fernidentifizierungssystems formuliert, nicht als Pflicht der Anwender („Betreiber"). Konkrete Vorgaben für die Ausgestaltung einer nationalen Rechtsgrundlage enthält die KI-Verordnung kaum; es wird lediglich festgelegt, dass sicherzustellen ist, dass die Strafverfolgungsbehörden keine ausschließlich auf der Grundlage der Ausgabe von Fernidentifizierungssystemen beruhende Entscheidung, aus der sich eine nachteilige Rechtsfolge für eine Person ergibt, treffen. Ein Genehmigungsvorbehalt gilt bei dem in dieser Arbeit vorrangig untersuchten Einsatzszenario der erstmaligen Identifizierung nicht.

C. Strafprozessrecht: Bestehen einer Rechtsgrundlage

Im nächsten Schritt ist zu untersuchen, ob im deutschen Strafprozessrecht eine Ermächtigung für den Einsatz automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger zu finden ist und ob diese den Anforderungen des Verfassungsrechts und des europäischen Rechts genügt. Eine Vorschrift, die ausdrücklich den Einsatz automatisierter Gesichtserkennung in der Strafverfolgung regelt, findet sich in der Strafprozessordnung nicht.

I. § 98c StPO

In der Praxis und auch in der Literatur wird § 98c StPO als taugliche Rechtsgrundlage zur Verwendung von Gesichtserkennung zur Identifizierung unbekannter Verdächtiger anhand von Lichtbilddatenbanken angesehen.[774]

Die Vorschrift des § 98c StPO regelt den sog. justizinternen Datenabgleich[775]: „Zur Aufklärung einer Straftat oder zur Ermittlung des Aufenthaltsortes einer Person, nach der für Zwecke eines Strafverfahrens gefahndet wird, dürfen personenbezogene Daten aus einem Strafverfahren mit anderen zur Strafverfolgung oder Strafvollstreckung oder zur Gefahrenabwehr gespeicherten Daten maschinell abgeglichen werden." (§ 98c S. 1 StPO). Anders als etwa bei der Rasterfahndung nach §§ 98a, b StPO[776] dürfen auf Grundlage des § 98c StPO personenbezogene Strafverfahrensdaten nur mit anderen zu repressiven oder präventiven Zwecken gespeicherten Daten abgeglichen werden, die bei Polizei oder Justiz bereits vorhanden („bevorratet") sind. Die Vorschrift wurde 1992 in die Strafprozessordnung eingeführt und sah sich von Anfang an erheblicher Kritik ausgesetzt,[777]

774 Mit ausführlicher Begründung *Schindler*, Biometrische Videoüberwachung, 2021, 425 ff., 547 f., der aber dennoch dafür plädiert, dass der Gesetzgeber eine spezifischere Vorschrift schafft. Siehe auch BT-Drs. 19/14952, 2; BT-Drs. 19/13796, 3; BeckOK StPO/*Gerhold*, 49. Ed., Stand: 1.10.2023, StPO § 98c Rn. 1; *Bauer/Gogoll/Zuber*, Gesichtserkennung, 2021, 51; *Hornung/Schindler*, DuD 2021, 515, 518; *Hornung/Schindler*, ZD 2017, 203, 207; *Petri*, GSZ 2018, 144, 148.

775 BeckOK StPO/*Gerhold*, 49. Ed., Stand: 1.10.2023, StPO § 98c Rn. 1; Satzger/Schluckebier/Widmaier/*Jäger*, StPO-Kommentar, 5. Aufl. 2023, § 98c StPO, Rn. 1; KK-StPO/*Greven*, 9. Aufl. 2023, StPO § 98c Rn. 1; SK-StPO/*Wohlers/Singelnstein*, 6. Aufl. 2023, § 98c StPO, Rn. 1. Näher zu § 98c StPO auch *Eckstein*, Ermittlungen zu Lasten Dritter, 2013, 292 ff.

776 Mitunter wird auch der Datenabgleich nach § 98c StPO als Rasterfahndung bezeichnet, siehe etwa *Siebrecht*, Rasterfahndung, 1997, 147 ff. („Rasterfahndung mit polizei-internen Daten"). Das Gesetz bezeichnet jedoch nur die Maßnahmen nach § 98a StPO als Rasterfahndung (amtliche Überschrift). Zur unterschiedlichen Verwendung des Begriffs auch BeckOK StPO/*Gerhold*, 49. Ed., Stand: 1.10.2023, StPO § 98a Rn. 2.

777 Kritisch bereits vor Einführung der Vorschrift *Hassemer*, KJ 1992, 64, 71 („unhaltbar") und *Crummenerl*, StV 1989, 131, 132 f.; vgl. auch MüKoStPO/*Hauschild*, 2. Aufl. 2023, StPO § 98c Rn. 1 („gesetzestechnisch missglückt"); *Siebrecht*, StV 1996, 566, 570 hält die Vorschrift für verfassungswidrig, da der Abgleich von Strafverfolgungsdaten mit Gefahrenabwehrdaten eine Zweckentfremdung darstelle, die Vorschrift des § 98c StPO jedoch „in keiner Weise" den verfassungsrechtlichen Anforderungen genüge, die an eine solche Zweckentfremdung zu stellen sind.

insbesondere da sie kaum Beschränkungen vorsieht. Dennoch ist die Vorschrift seitdem unverändert geblieben.

Maßnahmedaten[778] im Sinne des § 98c StPO („personenbezogene Daten aus einem Strafverfahren") sind alle personenbezogenen Daten, die im Rahmen eines Ermittlungsverfahrens prozessordnungsgemäß erhoben wurden.[779] Sie können etwa aus Zeugen- oder Beschuldigtenvernehmungen, strafprozessualen Zwangsmaßnahmen (z. B. Beschlagnahme) oder eingeholten Behördenauskünften (§§ 161, 163 StPO) stammen.[780] Nach der Gesetzesbegründung sollten insbesondere auch die im Strafverfahren nach § 34 Bundesmeldegesetz (BMG) aus dem Melderegister eingeholten Daten erfasst sein;[781] nach dieser Vorschrift darf die Meldebehörde der Strafverfolgungsbehörde beispielsweise Name, Geburtsdatum sowie die derzeitige und frühere Anschrift übermitteln. Diese personenbezogenen Daten kann die Strafverfolgungsbehörde dann etwa zum maschinellen Abgleich mit einer Fahndungsdatei verwenden. Maßnahmedaten beim Einsatz von Gesichtserkennung (das Suchbild) wären beispielsweise extrahierte Standbilder aus Videoaufzeichnungen (z. B. nach § 100h Abs. 1 Satz 1 Nr. 1 StPO).

Als Abgleichdaten können nach der insoweit offen formulierten Vorschrift des § 98c StPO alle anderen „zur Strafverfolgung oder Strafvollstreckung oder zur Gefahrenabwehr gespeicherten Daten" herangezogen werden. Besondere praktische Bedeutung hat vor allem das polizeiliche Informationssystem INPOL mit über 100 Teildatenbanken.[782] Dazu gehören auch sog. Gewalttäter- und Gefährderdateien, in denen auch Personen erfasst sind, deren Gefährlichkeit nur prognostiziert wird.[783] Es bestehen zudem Online-Verbindungen zum zentralen Verkehrsinformationssys-

778 So der Begriff von MüKoStPO/*Hauschild*, 2. Aufl. 2023, StPO § 98c Rn. 15; BeckOK StPO/*Gerhold*, 49. Ed., Stand: 1.10.2023, StPO § 98a Rn. 4 und KK-StPO/*Greven*, 9. Aufl. 2023, StPO § 98c Rn. 1 verwenden den Begriff „Strafverfahrensdaten".

779 Gemeint sind nur die Daten aus dem Ermittlungsverfahren, das Anlass für den Datenabgleich gibt. Vgl. hierzu MüKoStPO/Hauschild, 2. Aufl. 2023, StPO § 98c Rn. 13; BeckOK StPO/*Gerhold*, 49. Ed., Stand: 1.10.2023, StPO § 98c Rn. 4; Satzger/Schluckebier/Widmaier/*Jäger*, StPO-Kommentar, 5. Aufl. 2023, § 98c StPO, Rn. 3; weiter hingegen die Formulierung in BT-Drs. 12/989, 38: („Daten, die in einem Strafverfahren durch die in der Strafprozeßordnung geregelten Maßnahmen erhoben worden sind").

780 KK-StPO/*Greven*, 9. Aufl. 2023, StPO § 98c Rn. 1; MüKoStPO/*Hauschild*, 2. Aufl. 2023, StPO § 98c Rn. 15; Löwe/Rosenberg/*Menges* StPO, 27. Aufl. 2019, § 98c Rn. 5.

781 BT-Drs. 12/989, 38; siehe auch *Hilger*, NStZ 1992, 461 Fn. 76.

782 KK-StPO/*Greven*, 9. Aufl. 2023, StPO § 98c Rn. 2.

783 MüKoStPO/*Singelnstein*, Vorbemerkung zu § 483, 1. Aufl. 2019, Rn. 11.

tem (ZEVIS) des Kraftfahrt-Bundesamtes, zum Ausländerzentralregister (AZR) beim Bundesverwaltungsamt sowie zu Meldebehörden und Kfz-Zulassungsstellen der Länder.[784]

Abgeglichen werden dürfen personenbezogene Daten, also Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder aber bestimmbaren natürlichen Person.[785] Das sind beispielsweise Identifikationsmerkmale (wie Name, Anschrift und Geburtsdatum), äußere Merkmale (wie Geschlecht oder Größe) oder sonstige Informationen über eine Person wie strafrechtliche Verurteilungen oder vergangene oder laufende Ermittlungsverfahren.[786] Maßnahmen nach § 98c StPO können sich gegen den Beschuldigen richten, aber auch gegen Zeugen oder Sachverständige, etwa wenn deren Aufenthaltsort ermittelt werden soll.[787]

1. Materielle und formelle Voraussetzungen

Der maschinelle Datenabgleich nach § 98c StPO ist an keine besonderen Voraussetzungen geknüpft; er erfordert keine Katalogtat, keinen gesteigerten Tatverdacht, keine schriftliche Anordnung, keine richterliche Anordnung, keine Benachrichtigung des Betroffenen, keinen ausdrücklichen Vorrang weniger eingriffsintensiver Maßnahmen (Subsidiaritätsklausel).

784 *Müller*, Strafverfahrensrecht für Polizeistudium und -praxis, 2023, 310; *Soiné,* StPO, 144. Lieferung 2023, § 98c Rn. 5. Zu Recht kritisch hierzu BeckOK StPO/*Gerhold*, 49. Ed., Stand: 1.10.2023, StPO § 98c Rn. 5 mit dem Hinweis, dass diese Datenbestände jedenfalls nicht konkret für die geforderten Zwecke (Strafverfolgung, Strafvollstreckung, Gefahrabwehr), sondern allgemein zur Unterstützung aller möglichen Behörden gesammelt werden.

785 MüKoStPO/*Hauschild*, 2. Aufl. 2023, StPO § 98c Rn. 11. Zum Begriff der personenbezogenen Daten im Rahmen des Rechts auf informationelle Selbstbestimmung auch bereits Kapitel I. A. I. 1.

786 Vgl. nur BeckOK DatenschutzR/*Schild*, 46. Ed., Stand: 1.11.2023, DS-GVO Art. 4 Rn. 3.

787 *Soiné*, StPO, 144. Lieferung, 12/2023, § 98c Rn. 5; SK-StPO/*Wohlers/Singelnstein*, 6. Aufl. 2023, § 98c StPO, Rn. 2; *Eckstein*, Ermittlungen zu Lasten Dritter, 2013, 296.

a) Materielle Voraussetzung: Anfangsverdacht für (irgend-)eine Straftat

Voraussetzung für den maschinellen Datenabgleich ist lediglich ein Anfangsverdacht (§ 152 Abs. 2 StPO) für eine (beliebige) Straftat.[788] Es besteht keine Beschränkung auf Katalogtaten.

Auch ist § 98c StPO nicht gegenüber anderen Ermittlungsmaßnahmen subsidiär. Die meisten heimlichen Informationsbeschaffungsmaßnahmen wie etwa die Rasterfahndung (§§ 98a, b StPO), das Erstellen von Bildaufnahmen oder der Einsatz sonstiger besonderer für Observationszwecke bestimmter technischer Mittel (§ 100h Abs. 1 S. 1 Nr. 1 und 2 StPO) sind mit einer Subsidiaritätsklausel versehen und damit grundsätzlich nachrangig gegenüber weniger belastenden Eingriffen.[789] So darf die Rasterfahndung beispielsweise nur angeordnet werden, „wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Täters auf andere Weise erheblich weniger erfolgversprechend oder wesentlich erschwert wäre" (§ 98a Abs. 1 StPO). Dagegen ist der maschinelle Datenabgleich – und damit auch die Gesichtserkennung, wenn man sie unter die Vorschrift fassen würde – nicht ausdrücklich subsidiär gegenüber anderen weniger eingriffsintensiven Maßnahmen. Zwar gilt auch bei § 98c StPO wie bei jeder Ermittlungsmaßnahme der Verhältnismäßigkeitsgrundsatz. Eine Subsidiaritätsklausel ersetzt aber nicht die Verhältnismäßigkeitsprüfung, sondern stellt zusätzliche Anforderungen auf.[790] Während bei der Erforderlichkeit im Rahmen der Verhältnismäßigkeit nur *gleich* effektive Ermittlungsmaßnahmen verglichen werden, fragt die Subsidiaritätsklausel danach, ob alternative Ermittlungsmaßnahmen in einem bestimmten Maße *weniger* effektiv wären (z. B. „erheblich weniger erfolgversprechend oder wesentlich erschwert" bei § 98a Abs. 1 StPO oder „wesentlich erschwert oder aussichtslos" bei § 100a Abs. 1 StPO).[791] Zudem sind bei der Erforderlichkeitsprüfung

788 Satzger/Schluckebier/Widmaier/*Jäger*, StPO-Kommentar, 5. Aufl. 2023, § 98c StPO, Rn. 2; SK-StPO/ *Wohlers/Singelnstein*, 6. Aufl. 2023, § 98c StPO, Rn. 2; Löwe/Rosenberg/*Menges* StPO, 27. Aufl. 2019, § 98c Rn. 4.

789 *Riess*, in: GS Meyer, 1990, 367, 369; *Brodowski*, Verdeckte technische Überwachungsmaßnahmen im Polizei- und Strafverfahrensrecht, 2016, 195; siehe auch den Überblick bei *Blozik*, Subsidiaritätsklauseln im Strafverfahren, 2012, 91 f.

790 Vertiefend *Blozik*, Subsidiaritätsklauseln im Strafverfahren, 2012, 112 ff. Siehe auch *Bäcker*, Kriminalpräventionsrecht, 2015, 147. Anders wohl *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, 2023, 445.

791 *Bäcker*, Kriminalpräventionsrecht, 2015, 147 spricht daher davon, dass Subsidiaritätsregelungen zumeist gewisse „Effektivitätsverluste" der polizeilichen Tätigkeit hinnehmen.

die im konkreten Fall denkbaren Maßnahmen miteinander zu vergleichen, während eine Subsidiaritätsklausel abstrakt anordnet, dass eine Maßnahme nachrangig ist, unabhängig von ihrer Eingriffsintensität im konkreten Fall.[792]

b) Keine Verfahrensregeln oder Kontrollmechanismen

Die Vorschrift des § 101 StPO regelt einheitlich für die meisten[793] verdeckten Maßnahmen die (getrennte) Aktenführung (Abs. 1), die Kennzeichnung der aufgrund dieser Maßnahmen erhobenen personenbezogenen Daten (Abs. 3), maßnahmenspezifisch die Benachrichtigung der Betroffenen (Abs. 4), die Voraussetzungen für eine zeitweise Zurückstellung dieser Benachrichtigung (Abs. 5), die gerichtliche Überprüfung der Zurückstellung (Abs. 6, 7) und die Löschung der durch die Maßnahmen erlangten personenbezogenen Daten (Abs. 8). Die Vorschrift des § 98c StPO hat der Gesetzgeber jedoch nicht in § 101 StPO aufgenommen, sodass diese Verfahrensvorgaben bei einem entsprechenden maschinellen Datenabgleich nicht gelten.

Das Erfordernis einer schriftlichen Anordnung bei der Rasterfahndung (§ 98b Abs. 1 S. 4 und 5 StPO) gilt nicht für § 98c StPO, sodass der maschinelle Datenabgleich mündlich angeordnet werden darf.

Beim Einsatz neuartiger technischer Eingriffsinstrumente wie der automatisierten Gesichtserkennung erscheint eine Beobachtung, Kontrolle und Evaluation unverzichtbar. Art. 64 Abs. 2 S. 2 BayPAG sieht für den polizeilichen Einsatz von Gesichtserkennung nach Art. 61 Abs. 2 BayPAG vor, dass eine Datenschutz-Folgenabschätzung vorzunehmen ist. Ob eine solche den Risiken, welche die automatisierte Gesichtserkennung birgt, ausreichend begegnet, ist zwar fraglich; schließlich stellen sich Probleme der Fehleranfälligkeit und potenziellen Diskriminierung, die eine „Datenschutzanalyse" nicht hinreichend abbilden würde.[794] § 98c StPO sieht aber nicht einmal eine solche Datenschutz-Folgenabschätzung vor.[795] Dies mag für die übli-

792 *Bäcker*, Kriminalpräventionsrecht, 2015, 147; *Riess*, in: GS Meyer, 1990, 367, 372.

793 Siehe aber § 101a StPO, der Verfahrensvorschriften für Maßnahmen nach § 100g StPO regelt.

794 Hierzu auch bereits Kapitel II. A. 3. c) cc).

795 Eine Datenschutz-Folgenabschätzung dürfte bei der automatisierten Gesichtserkennung zwar bereits wegen § 67 BDSG, Art. 27 JI-RL erforderlich sein; vgl. auch *Europäischer Datenschutzausschuss*, Guidelines 05/2022 on the use of facial recognition

chen Maßnahmen, die auf die Vorschrift gestützt werden, auch nicht erforderlich sein. Beim Einsatz automatisierter Gesichtserkennung wären solche Mechanismen jedoch nötig.

Im Übrigen würde § 98c StPO auch nicht vorschreiben, dass und wie eine menschliche Kontrolle von Gesichtserkennungstreffern erfolgen muss. Ließe man es zu, den Einsatz automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger auf § 98c StPO zu stützen, dann ist es jeder beliebigen Landespolizeibehörde auch erlaubt, ein eigenes Gesichtserkennungssystem anzuschaffen, damit ihren lokalen Lichtbildbestand zu durchsuchen und einem beliebigen, nicht hierfür gesondert ausgebildeten Polizisten die Aufgabe zu übertragen, aus der Kandidatenliste den Verdächtigen auszuwählen, gegen den nun weiter ermittelt werden soll.

c) Fazit

Voraussetzung für eine Maßnahme nach § 98c StPO ist lediglich ein Anfangsverdacht für (irgend-)eine Straftat. Die Eingriffsschwelle ist daher denkbar niedrig.[796] *Körffer* bezeichnete die Vorschrift treffend als „materiell weitgehend und formell vollständig voraussetzungslos".[797] Vor diesem Hintergrund wird davon ausgegangen, dass die Vorschrift nur geringfügige Grundrechtseingriffe legitimieren kann.[798] Ein auf Basis automatisierter

technology in the area of law enforcement, Version 2.0, 2023, 7, 26 f. Es ist allerdings nicht bekannt, ob und unter welchen Umständen eine solche vorgenommen wird. Auch deswegen dürfte es sinnvoll sein, Fallgruppen, in denen eine Datenschutz-Folgenabschätzung vorzunehmen ist, in § 76 BDSG festzulegen (wie bei Art. 35 Abs. 3 DSGVO) oder das Erfordernis der Datenschutz-Folgenabschätzung in der jeweiligen strafprozessualen Rechtsgrundlage zu verankern.

796 Vgl. zur geringen Eingriffsschwelle auch *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, 2023, 10; Satzger/Schluckebier/Widmaier/*Jäger*, StPO-Kommentar, 5. Aufl. 2023, § 98c StPO, Rn. 1; BeckOK StPO/*Gerhold*, 49. Ed., Stand: 1.10.2023, StPO § 98c Rn. 1; KK-StPO/*Greven*, 9. Aufl. 2023, StPO § 98c Rn. 1; *Hornung/Schindler*, ZD 2017, 203, 207 und Fn. 30; *Körffer*, DANA 2014, 146, 148; *Singelnstein*, NStZ 2012, 593, 606; *Hilger*, NStZ 1992, 457, 461.

797 *Körffer*, DANA 2014, 146, 148; zustimmend BeckOK StPO/*Gerhold*, 49. Ed., Stand: 1.10.2023, StPO § 98c Rn. 1; *Gercke*, in: Gercke/Temming/Zöller, Strafprozessordnung, 7. Aufl. 2023, § 98c StPO Rn. 3; VGH Mannheim, NVwZ-RR 2019, 901, 903.

798 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, 2023, 10; BeckOK StPO/*Gerhold*, 49. Ed., Stand: 1.10.2023, StPO § 98c Rn. 1; *Gercke*, in: Gercke/Temming/Zöller, Strafprozessordnung, 7. Aufl. 2023, § 98c StPO Rn. 3; *Körffer*, DANA 2014, 146, 148; vgl. auch *Kudlich*, JuS 2001, 1165, 1167 und Fn. 18; *Bernsmann/Jansen*,

Gesichtserkennung vorgenommener Abgleich von Lichtbildern zur Identifizierung unbekannter Verdächtiger ist jedoch kein geringfügiger, sondern ein erheblicher Grundrechtseingriff. Dies ergibt sich, wie oben ausführlich herausgearbeitet, aus der Kombination von Heimlichkeit, Streubreite, Anlasslosigkeit, Anknüpfung an höchstpersönliche Merkmale, Möglichkeit der Verknüpfung, drohenden Nachteilen und spezifischer Fehleranfälligkeit der Maßnahme.[799] Ein solcher Eingriff kann daher nicht auf § 98c StPO gestützt werden.

2. Bestimmtheit und Normenklarheit

Zudem genügt die Vorschrift des § 98c StPO nicht den Anforderungen des Gebots der Bestimmtheit und der Normenklarheit, die beim Einsatz von Gesichtserkennung zur Identifizierung unbekannter Verdächtiger an eine Rechtsgrundlage zu stellen sind. Anlass, Zweck und Grenzen des Eingriffs müssten bereichsspezifisch, präzise und normenklar festgelegt werden. Wie bereits herausgearbeitet,[800] sind vor dem Hintergrund des erheblichen Eingriffsgewichts und insbesondere der Heimlichkeit der Gesichtserkennung erhöhte Anforderungen an Bestimmtheit und Normenklarheit zu stellen. Nur so können Eingriffsbefugnisse wirksam begrenzt und eine effektive gerichtliche Kontrolle ermöglicht werden. Zudem kann nur durch eine ausreichende Bestimmtheit der Vorschrift sichergestellt werden, dass der demokratisch legitimierte Gesetzgeber die wesentlichen Entscheidungen über Grundrechtseingriffe und deren Reichweite selbst trifft. Mit Blick auf Gesichtserkennung müsste der Gesetzgeber also zumindest die Entscheidung treffen, welche der vielen möglichen Einsatzszenarien zugelassen werden sollen und welche nicht (Anlass und Zweck des Eingriffs), und die grundsätzliche Ausgestaltung (Grenzen) dieser Maßnahmen vornehmen.

StV 1998, 217, 222. Nicht ganz eindeutig *Müller/Schwabenbauer*, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, G. Informationsverarbeitung im Polizei- und Strafverfahrensrecht, Rn. 933, die zutreffend argumentieren, dass der in einem Datenabgleich liegende Grundrechtseingriff nicht pauschal deshalb als geringfügig anzusehen ist, weil die Daten bereits bevorratet waren; es wird jedoch nicht ganz deutlich, ob bei einem (im Einzelfall) erheblichen Grundrechtseingriff die allgemeine Vorschrift zum Datenabgleich dennoch herangezogen werden kann oder nicht.

799 Kapitel II. A. I. 2. b).

800 Kapitel II. A. I. 3. b).

Bei heimlichen Maßnahmen wie der Gesichtserkennung muss der Inhalt der einzelnen Norm auch deshalb verständlich und ohne größere Schwierigkeiten durch Auslegung zu konkretisieren sein, weil hier die Grundrechte ohne Wissen der Bürger und oft ohne die Erreichbarkeit gerichtlicher Kontrolle eingeschränkt werden. Die Rechtsgrundlage muss, mit den Worten *Bäckers* gesprochen, selbst bereits eine „erhebliche Konkretisierungsleistung erbringen".[801]

Daher wurden oben folgende Anforderungen an die Bestimmtheit und Normenklarheit herausgearbeitet: Die Rechtsgrundlage muss deutlich machen, dass ein automatisierter Abgleich von Daten durchgeführt wird, welche Arten von Daten abgeglichen werden dürfen (bei den für die Embeddings extrahierten Gesichtsmerkmalen handelt es sich um höchstpersönliche Merkmale), welche Datensätze abgeglichen werden dürfen (also welche polizeilichen Datenbanken herangezogen werden dürfen) und zu welchem genauen Zweck der Abgleich erfolgen darf (z. B. Gesichtserkennungsabgleich zur Identifizierung unbekannter Verdächtiger, nicht aber zur Echtzeit-Fahndung).[802] Vor dem Hintergrund dieser Anforderungen ist § 98c StPO auch im Hinblick auf Bestimmtheit und Normenklarheit keine taugliche Ermächtigung für den Einsatz automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger anhand von Lichtbilddatenbanken.

a) Weit formulierter Zweck („zur Aufklärung einer Straftat")

Bereits der Zweck und Anlass für den Gesichtserkennungsabgleich würde nicht aus der Rechtsgrundlage deutlich. § 98c StPO erlaubt einen Datenabgleich zur Aufklärung einer Straftat oder zur Ermittlung des Aufenthaltsortes einer Person. Würde man den Einsatz automatisierter Gesichtserkennung auf Basis dieser Vorschrift zulassen, bliebe unklar, welche der verschiedenen Einsatzszenarien erlaubt sein sollen und welche nicht. Das wird bereits daran deutlich, dass der Wortlaut des § 98c StPO auch die Auswertung umfangreichen Datenmaterials per Gesichtserkennung („zur Aufklärung von Straftaten"), die digitale Beobachtung, womöglich sogar die Personenfahndung im öffentlichen Raum per Gesichtserkennung („zur

801 *Bäcker*, in: Herdegen/Masing/Poscher/Gärditz, Handbuch des Verfassungsrechts, 2021, § 28 Sicherheitsverfassungsrecht, Rn. 87.

802 Kapitel II. A. I. 3. b).

Ermittlung des Aufenthaltsortes einer Person") erfassen würde. Denn bei der Auswertung umfangreichen Datenmaterials per Gesichtserkennung wie nach den G20-Ausschreitungen erfolgte schließlich auch ein Abgleich von Strafverfahrensdaten (Bild der Person, über deren Taten oder Vor- und Nachtatverhalten weitere Informationen generiert werden sollen) mit anderen zur Gefahrenabwehr oder Strafverfolgung gespeicherten Daten (z. B. staatliche und private Videoaufzeichnungen des aufzuklärenden komplexen Sachverhalts). Zur digitalen Beobachtung einer Person könnte ihr Bild (Strafverfahrensdatum) mit Aufzeichnungen aus dem öffentlichen Raum abgeglichen werden (die zur Gefahrenabwehr gespeichert wurden), um weitere Informationen herauszufinden. Auch könnte man argumentieren, dass bei der Personenfahndung im öffentlichen Raum per Gesichtserkennung ebenfalls Strafverfahrensdaten (Bild der gesuchten Person) mit Gefahrenabwehrdateien (Videoaufzeichnungen im öffentlichen Raum) abgeglichen werden.[803] Sollen all diese Szenarien wirklich von § 98c StPO erfasst sein?[804] Die Vorschrift zieht hier jedenfalls keine eindeutigen Grenzen. Anlass und Zweck eines Einsatzes automatisierter Gesichtserkennung wären so höchst unbestimmt und wenig normenklar geregelt.

Da Datenabgleiche nach § 98c StPO im Übrigen nicht auf den Beschuldigten beschränkt sind, sondern auch Zeugen oder Sachverständige betreffen könnten, müsste also auch der Einsatz von Gesichtserkennung zur Identifizierung von Zeugen auf diese Vorschrift gestützt werden können.

803 Wobei man hier zumindest einwenden könnte, dass eine Fahndung in Echtzeit nicht unter § 98c StPO fallen kann, weil dies eine unzulässige Kombination zweier Rechtsgrundlagen (Anfertigung der Aufzeichnung einerseits und Abgleich andererseits) wäre; zu diesem Gedanken *Schindler*, Biometrische Videoüberwachung, 2021, 547, 536 f.; vgl. auch *Hornung/Schindler*, ZD 2017, 203, 208.

804 Einhellig wird davon ausgegangen, dass die Personenfahndung im öffentlichen Raum nicht auf § 98c StPO (oder eine sonstige bereits existierende Rechtsgrundlage) gestützt werden kann, siehe etwa BeckOK StPO/*Gerhold*, 49. Ed., Stand: 1.10.2023, StPO § 98c Rn. 1; *Gercke*, in: Gercke/Temming/Zöller, Strafprozessordnung, 7. Aufl. 2023, § 98c StPO Rn. 3; *Martini*, NVwZ-Extra 1-2/2022, 1, 10 f.; *Schindler*, Biometrische Videoüberwachung, 2021, 536 f.; *Bauer/Gogoll/Zuber*, Gesichtserkennung, 2021, 41; *Hornung/Schindler*, ZD 2017, 203, 208 f.; *Petri*, GSZ 2018, 144, 147 f. Mit Blick auf die Auswertung von umfangreichem Datenmaterial per Gesichtserkennung wird überwiegend § 98c StPO als Rechtsgrundlage abgelehnt und gefordert, dass eine Spezialrechtsgrundlage geschaffen werden müsse, so etwa *Bauer/Gogoll/Zuber*, Gesichtserkennung, 2021, 50; vgl. auch BeckOK StPO/*Gerhold*, 49. Ed., Stand: 1.10.2023, StPO § 98c Rn. 1; *Gercke*, in: Gercke/Temming/Zöller, Strafprozessordnung, 7. Aufl. 2023, § 98c StPO Rn. 3; *Fährmann*, MMR 2020, 228, 232; anders *Schindler*, Biometrische Videoüberwachung, 2021, 550, 732, der aber auch hier für spezifischere Regelungen plädiert.

Private könnten dann also auch Bildaufnahmen eines Deliktsgeschehens bei der Polizei einreichen, die dann die Identität der im Hintergrund stehenden Zeugen ermitteln könnte. Es kann wohl kaum gewollt sein, dass solche Gesichtserkennungsrecherchen mit Blick auf Dritte auf eine generalklauselartige Vorschrift gestützt werden; hier müsste der Gesetzgeber tätig werden.

b) Keine nähere Bezeichnung des technischen Eingriffsinstruments

Weiterhin ist zu fragen, welche Art von Auswertungen der Begriff des „maschinellen Abgleichs" in § 98c StPO zulässt.[805] Ist es mit dem Bestimmtheitsgrundsatz vereinbar, dass das technische Eingriffsinstrument – die automatisierte Gesichtserkennung – aus § 98c StPO nicht ersichtlich wird. Mit anderen Worten: Wie „technikoffen"[806] darf eine Eingriffsnorm formuliert sein?

Mit einer solchen Frage befasste sich das Bundesverfassungsgericht im Jahr 2005 im Hinblick auf die Verwendung des GPS (Global Positioning System).[807] Die Rechtsgrundlage sah vor, dass „besondere für Observationszwecke bestimmte technische Mittel" zur Erforschung des Sachverhalts oder zur Ermittlung des Aufenthaltsortes des Täters eingesetzt werden dürfen (§ 100c Abs. 1 Nr. 1 lit. b StPO a. F.). Das Bundesverfassungsgericht sah es als mit dem Bestimmtheitsgebot vereinbar, die Verwendung des GPS auf diese Ermächtigung zu stützen.[808] Das Bestimmtheitsgebot verlange vom Gesetzgeber, dass er technische Eingriffsinstrumente genau bezeichne und dadurch sicherstelle, dass der Adressat den Inhalt der Norm jeweils erkennen könne.[809] Erforderlich seien aber keine gesetzlichen Formulierungen, die „jede Einbeziehung kriminaltechnischer Neuerungen ausschließen".[810] Allerdings habe der Gesetzgeber wegen des schnellen und für den Grundrechtsschutz riskanten informationstechnischen Wandels die technischen Entwicklungen aufmerksam zu beobachten und bei Fehlentwicklungen

805 Vgl. auch *Körffer*, DANA 2014, 146, 149.
806 Zur „Technikoffenheit" strafprozessualer Ermittlungsbefugnisse siehe *Roggan*, NJW 2015, 1995; vgl. zum Gefahrenabwehrrecht *Golla*, in: Chibanguza/Kuß/Steege, Künstliche Intelligenz, 2022, 2. Teil: § 9 A. KI-Einsatz bei der Polizei Rn. 20 ff.
807 BVerfGE 112, 304.
808 BVerfGE 112, 304 (317).
809 BVerfGE 112, 304 (316).
810 BVerfGE 112, 304 (316).

hinsichtlich der konkreten Ausfüllung offener Gesetzesbegriffe durch die Strafverfolgungsbehörden und die Strafgerichte notfalls durch ergänzende Rechtssetzung korrigierend einzugreifen.[811] Mit Blick auf den Einsatz des GPS war das Bundesverfassungsgericht der Auffassung, dass die Verwendung des Merkmals „besondere für Observationszwecke bestimmte technische Mittel" diesen Anforderungen gerecht werde. Denn was damit gemeint ist, sei in seiner Zielrichtung leicht verständlich und lasse sich mit den anerkannten Methoden der Gesetzesauslegung konkretisieren.[812] Durch die systematische Abgrenzung zu den in § 100c Abs. 1 Nr. 1 lit. a StPO (a. F.) genannten Mitteln einfacher optischer Überwachungstätigkeit einerseits und den durch § 100c Abs. 1 Nrn. 2 und 3 StPO (a. F.) geregelten akustischen Überwachungs- und Aufzeichnungstechniken andererseits habe der Gesetzgeber einen Bereich hinreichend bestimmt abgegrenzt, in dem moderne Kriminaltechnik zur Anwendung kommen dürfe, die in anderer Weise die weitere Aufklärung des Sachverhalts oder die Ortung einer Person möglich mache.[813] Es gehe um Ortung und Aufenthaltsbestimmung durch Beobachtung mit technischen Mitteln. Innerhalb dieses Bereichs halte sich die Verwendung des GPS. Gegenüber den ebenfalls erfassten Bewegungsmeldern und Nachtsichtgeräten zeichne sich das GPS zwar durch eine verbesserte Flexibilität im Einsatz und eine erhöhte Genauigkeit der Ergebnisse aus. Andererseits unterliege aber auch das GPS aufgrund seiner technischen Spezifikation Beschränkungen beim Empfang in geschlossenen Räumen oder innerhalb von Häuserschluchten. Bei dieser Sachlage habe der Gesetzgeber nicht davon ausgehen müssen, dass das GPS zu einem Observationsinstrument besonderer Art und spezifischer Tiefe werden könnte, dessen Einsatz von Verfassungs wegen nur unter restriktiveren Voraussetzungen gestattet werden dürfe.[814]

Bei § 98c StPO ist das technische Eingriffsinstrument der „maschinelle Datenabgleich". Ausweislich der Gesetzesbegründung aus dem Jahr 1991 hat die Vorschrift „insbesondere den Abgleich des Fahndungstatbestands mit den Dateien der Einwohnermeldeämter vor Augen".[815] Bei einem Abgleich wie ihn sich die Gesetzesbegründung vorgestellt hat, werden also vor allem Wörter (oder Zahlen) maschinell abgeglichen. Eine solche Recherche

811 BVerfGE 112, 304 (316).
812 BVerfGE 112, 304 (317).
813 BVerfGE 112, 304 (317).
814 BVerfGE 112, 304 (317).
815 BT-Drs. 12/989, 38.

liefert regelmäßig eine klare Antwort. Wird etwa anhand von Meldedaten die frühere Anschrift einer zur Fahndung ausgeschriebenen Person recherchiert, liefert die Suche ein eindeutiges Ergebnis (die frühere Anschrift oder das eindeutige Ergebnis, dass keine Informationen vorhanden sind). Auch wenn beispielsweise anhand eines maschinellen Abgleichs nachgeforscht wird, ob sich ein Name in einer Datenbank befindet, dann kann dies mit einem klaren „Ja" oder „Nein" beantwortet werden. Besondere Fähigkeiten, um dieses Ergebnis zu interpretieren, sind nicht erforderlich.[816]

Nicht so bei der Gesichtserkennung; hier ist das Suchergebnis uneindeutig und diffus, sodass eine wirksame und sachkundige menschliche Überprüfung angezeigt ist. Dass eine solche automatisierte Recherche nach „ähnlichen" Gesichtern getätigt werden darf, lässt § 98c StPO mit der Formulierung „Daten abgleichen" aber nicht ausreichend erkennen. Im Übrigen ist die bei einer solchen Abfrage erforderliche menschliche Kontrolle der Ergebnisse in dieser Vorschrift in keiner Weise geregelt. Damit kann der Einsatz automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger auch bereits deshalb nicht auf § 98c StPO gestützt werden, weil dieser nicht ausreichend deutlich macht, dass ein solches technisches Eingriffsinstrument – das uneindeutige, interpretationsbedürftige Ergebnisse generiert – eingesetzt werden dürfte.

In eine ähnliche Richtung geht die Auffassung des Bundesverfassungsgerichts im Zusammenhang mit Abfragen und Recherchen in der Antiterrordatei nach § 5 Antiterrordateigesetz (ATDG).[817] Diese Vorschrift ist ohne besondere Eingriffsschwellen ausgestaltet und erlaubt es den beteiligten Behörden, „die in der Antiterrordatei gespeicherten Daten im automatisierten

816 In eine ähnliche Richtung gehen die Überlegungen bei *Körffer*, DANA 2014, 146, 149 („Zwischen einer einfachen Suchanfrage nach dem Namen einer Person in einer Datenbank und einer komplexen Auswertung, die eventuell auch selbstlernend nach übereinstimmenden Mustern sucht, bestehen im Hinblick auf die Grundrechtsgefährdung erhebliche Unterschiede."). Vgl. auch die überzeugenden Gedanken von *Rückert* dahingehend, dass § 98c StPO keine taugliche Rechtsgrundlage für Data Mining ist *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, 2023, 10 f., 409 f. Er sieht die Grenze des § 98c StPO dort, „wo nicht nur deterministische Methoden eingesetzt werden, um unzweifelhaft in den abgeglichenen Datensätzen enthaltene Informationen zu Tage zu fördern, sondern statistische Methoden und insbesondere selbstlernende Verfahren eingesetzt werden, um neue Informationen zu Tage zu fördern, die nicht unzweifelhaft in den Datensätzen enthalten sind, sondern aus dem Abgleich gleichermaßen vom Algorithmus „geschlussfolgert" werden".

817 BVerfGE 133, 277 (361). Siehe auch jüngst zu § 6a ATDG BVerfGE 165, 363 (404, 436).

Verfahren [zu] nutzen" und hierfür Abfragen vorzunehmen.[818] Das Bundesverfassungsgericht sah die Vorschrift als verfassungskonform an, da eine Grenze des § 5 ATDG insbesondere darin liege, dass nur Einzelabfragen, nicht aber auch „eine Rasterung, Sammelabfragen oder die übergreifende Ermittlung von Zusammenhängen zwischen Personen durch Verknüpfung von Datenfeldern erlaubt" seien.[819] In ihrer derzeitigen Ausgestaltung ermächtige die Vorschrift aber „weder zu einer automatischen Bilderkennung noch zur Verwendung von Ähnlichenfunktionen oder zur Abfrage mit unvollständigen Daten (so genannten „wildcards")".[820]

c) Keine ausreichende Begrenzung der Datenbanken

Da nach § 98c StPO alle „zur Strafverfolgung oder Strafvollstreckung oder zur Gefahrenabwehr gespeicherten Daten" zum Abgleich herangezogen werden dürfen, wären auch die Datenbanken, die per Gesichtserkennung durchsucht werden dürften, wenig bestimmt geregelt. Die fehlende nähere Begrenzung der Datenbanken wird mit Blick auf § 98c StPO ohnehin als problematisch angesehen.[821] Beim Einsatz automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger gilt das umso mehr. Denn diese Maßnahme birgt immer die Gefahr von Fehlidentifizierungen und jeder, der sich in einer per Gesichtserkennung durchsuchbaren Datenbank befindet, könnte fälschlicherweise von dem Gesichtserkennungssystem auf die Kandidatenliste gesetzt und fälschlicherweise von einem Menschen als der Verdächtige erkannt oder zumindest vermutet werden. Dann schließen sich weitere Ermittlungsmaßnahmen gegen diese Person an. Die Entscheidung, welche Datenbanken – also welche Personen – überhaupt in

818 Die Vorschrift des § 5 ATDG gilt heute weiterhin weitgehend inhaltsgleich.

819 BVerfGE 133, 277 (361).

820 BVerfGE 133, 277 (361); hierzu auch *Golla*, in: Dietrich/Fahrner/Gazeas/von Heintschel-Heinegg, Handbuch Sicherheits- und Staatsschutzrecht, 2022, § 30 Kooperative Informationsressourcen, Rn. 92. Wildcards sind Sonderzeichen, die als Platz für unbekannte Zeichen stehen und mit denen ähnliche, aber nicht identische Daten gefunden werden können: Die Suche nach „Schmi*" liefert etwa auch die Ergebnisse „Schmidt", „Schmitt" und „Schmied". Was das Bundesverfassungsgericht mit einer „automatischen Bilderkennung" meint, ergibt sich aus der Entscheidung nicht; es liegt aber nahe, dass dies auch die automatisierte Gesichtserkennung betrifft.

821 Kritisch BeckOK StPO/*Gerhold*, 49. Ed., Stand: 1.10.2023, StPO § 98c Rn. 5; vgl. auch *Fährmann*, in: Grafl/Stempkowski/Beclin/Haider, „Sag, wie hast du's mit der Kriminologie?" Die Kriminologie im Gespräch mit ihren Nachbardisziplinen, 2020, 643, 650; *Aden/Fährmann*, ZRP 2019, 175, 178.

den Abgleich einbezogen werden, ist daher potenziell folgenreich. Anders ist dies, wenn im Rahmen des § 98c StPO nur ein klassischer Datenabgleich von Wörtern oder Zahlen erfolgt, der eindeutige Ergebnisse liefert.

Realitätsnah muss zudem im Hinterkopf behalten werden, dass ein mächtiges Ermittlungswerkzeug wie die automatisierte Gesichtserkennung auch neue Begehrlichkeiten wecken kann. Je mehr Personen in einer Lichtbilddatenbank gespeichert sind, desto wahrscheinlicher ist es, dass sich der unbekannte Verdächtige in einem künftigen Ermittlungsverfahren unter ihnen befindet. Strafverfolgungsbehörden haben so den Anreiz, Lichtbilder von mehr und mehr Personen in ihren Datenbanken zu erfassen. Eine wirksame Begrenzung der Datenbanken durch den Gesetzgeber ist daher erforderlich.[822]

Dem steht auch nicht entgegen, dass das Bundesverfassungsgericht in seiner Entscheidung zur automatisierten Kfz-Kennzeichenkontrolle es als vereinbar mit dem Bestimmtheitsgrundsatz angesehen hat, dass die Rechtsgrundlage die zum Abgleich zugelassenen Fahndungsbestände „nur abstrakt, nicht aber unter Verweis auf konkrete Dateien" umschrieb.[823] Die entsprechende Regelung (Art. 33 Abs. 2 S. 2 BayPAG a. F.) lautete „Zulässig ist der Abgleich der Kennzeichen mit polizeilichen Fahndungsbeständen, die erstellt wurden 1. über Kraftfahrzeuge oder Kennzeichen, die durch Straftaten oder sonst abhandengekommen sind, 2. über Personen, die ausgeschrieben sind a) zur polizeilichen Beobachtung, gezielten Kontrolle oder verdeckten Registrierung, b) aus Gründen der Strafverfolgung, Strafvollstreckung, Auslieferung oder Überstellung, c) zum Zweck der Durchführung ausländerrechtlicher Maßnahmen, d) wegen gegen sie veranlasster polizeilicher Maßnahmen der Gefahrenabwehr".[824] In dieser abstrakten Umschreibung der Fahndungsbestände liege weder eine unzulässige dynamische Verweisung, noch widerspreche dies dem Bestimmtheitsgebot.[825] Vielmehr habe der Gesetzgeber damit eine hinreichend klare Entscheidung

822 *Schindler* ist zwar der Auffassung, dass § 98c StPO den Bestimmtheitsanforderungen für den Einsatz automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger anhand von Lichtbilddatenbanken genügt. Gleichwohl hält er eine „stärkere Eingrenzung der für den Abgleich heranzuziehenden Datenbestände in den jeweiligen Vorschriften" für wünschenswert, siehe *Schindler*, Biometrische Videoüberwachung, 2021, 547 f.

823 BVerfGE 150, 244 (288).

824 Die Regelung findet sich heute weitgehend inhaltsgleich (bis auf Abs. 1 Nr. 1 b)) in Art. 39 BayPAG.

825 BVerfGE 150, 244 (288).

getroffen, deren Gehalt sich durch Auslegung ermitteln lasse und die den Zugriff auf die nicht speziell auf die Kennzeichenkontrolle hin angelegten Fahndungsbestände sachbezogen eingrenze.[826] Auf ihrer Grundlage dürfe die nähere Auswahl aus den genannten Fahndungsbeständen den Behörden überlassen werden, die sie nach pflichtgemäßem Ermessen und unter der Berücksichtigung des Verhältnismäßigkeitsprinzips vorzunehmen hätten.[827] Dass ihnen hierbei eine gewisse Einschätzungsprärogative eingeräumt werde, sei verfassungsrechtlich nicht ausgeschlossen.[828] Diese gesetzgeberische Eingrenzung der zum Abgleich zugelassenen Daten ist aber deutlich stärker als bei § 98c StPO, denn es dürfen ohnehin nur *Fahndungsbestände* herangezogen werden und nicht, wie bei beim maschinellen Datenabgleich sämtliche Daten, die zur Strafverfolgung, Strafvollstreckung oder Gefahrenabwehr gespeichert sind.[829] Auch sei erneut daran erinnert, dass bei der automatisierten Kfz-Kennzeichenkontrolle die Gefahr einer Fehlidentifizierung beinahe inexistent ist, da falsche Treffer eindeutig erkannt und aussortiert werden können. Im Übrigen sind bei der Kfz-Kennzeichenkontrolle zwar personenbezogene Daten (Kennzeichen) betroffen, nicht hingegen – wie bei der Gesichtserkennung – biometrische und sogar höchstpersönliche, unveränderliche Merkmale. Eine Begrenzung der zum Abgleich zugelassenen Datenbestände ist angesichts der Fehleranfälligkeit und Sensibilität der Daten daher noch wichtiger.

d) Keine ausdrückliche Nennung biometrischer Merkmale

Dies führt auch schon zum nächsten Kritikpunkt mit Blick auf die fehlende Bestimmtheit des § 98c StPO als Grundlage für eine automatisierte Gesichtserkennung. Die Vorschrift lässt nicht erkennen, dass *biometrische* Daten verarbeitet werden. Eine ausdrückliche Nennung der zu verarbeitenden Daten wäre aber wegen des verfassungsrechtlichen Grundsatzes der

826 BVerfGE 150, 244 (288).
827 BVerfGE 150, 244 (288 f.).
828 BVerfGE 150, 244 (289).
829 Man könnte auch argumentieren, dass die Fahndungsbestände bei der automatisierten Kennzeichenkontrolle eher den Maßnahmedaten (als den Abgleichdaten) beim maschinellen Datenabgleich nach § 98c StPO entsprechen und die vorbeifahrenden Kraftfahrzeuge den Abgleichdaten. Die vorbeifahrenden Kraftfahrzeuge können aber bei einer Maßnahme wie der automatisierten Kfz-Kontrolle kraft Natur der Sache gar nicht begrenzt werden.

Bestimmtheit und Normenklarheit geboten,[830] jedenfalls folgt dieses Erfordernis aus Art. 8 Abs. 2 JI-RL[831].

Bei den für die Embeddings extrahierten Gesichtsmerkmalen handelt es sich nicht nur um personenbezogene, sondern um biometrische, darüber hinaus höchstpersönliche Daten, die außerdem noch weitgehend unveränderlich und individuell sind und einem Menschen immer und überall hin „folgen". Personenbezogene Daten sind hingegen etwa auch Name, Anschrift, Geschlecht, Familienstand und Vorstrafen. Höchstpersönliche, individuelle Merkmale wie die Gesichtsgeometrie sind besonders sensible Daten, da sie eine sekundenschnelle Zuordnung und Wiedererkennung in unzähligen Datensätzen ermöglichen. Sie machen die entsprechende Person immer und überall auffindbar und all ihre Fotos verknüpfbar. Die Suche in einer Datenbank anhand eines Namens ist damit nicht zu vergleichen. Der Name oder andere personenbezogene Daten einer Person sind auch nicht nach außen erkennbar; das Gesicht lässt sich dagegen nicht verbergen und ein Foto einer Person lässt sich auch heimlich anfertigen. Dass solche sensiblen Daten im Rahmen einer Strafverfolgungsmaßnahme verwendet werden dürfen, muss der Gesetzgeber entscheiden und diese Entscheidung dann eindeutig aus dem Gesetz hervorgehen.[832]

So sieht beispielsweise Art. 61 Abs. 2 BayPAG, der insbesondere den Einsatz von Gesichtserkennungssoftware erlauben soll,[833] vor, dass der Abgleich personenbezogener Daten „auch unter Verwendung bildverarbeitender Systeme und durch Auswertung biometrischer Daten erfolgen" kann. Eine solch konkrete Benennung der zum Abgleich zugelassenen Daten ist vor dem Hintergrund des Bestimmtheitsgrundsatzes auch geboten. § 98c StPO spricht jedoch nur von „personenbezogenen Daten".

e) Fazit

Die Vorschrift des § 98c StPO wird auch mit Blick auf die Bestimmtheit und Normenklarheit nicht den Anforderungen gerecht, die eine Ermächtigung

830 Kapitel II. A. I. 3. b) und Kapitel II. C. I. 2. d).
831 Kapitel II. B. I. 2. a).
832 So wohl auch *Martini*, NVwZ-Extra 1-2/2022, 1, 11. *Schindler* hält es zwar nicht für zwingend, aber doch zumindest für „vorzugswürdig", dass die Verwendung biometrischer Daten in einer Rechtsgrundlage erwähnt werden, siehe *Schindler*, Biometrische Videoüberwachung, 2021, 547 f.
833 Siehe BayLT-Drs.17/20425, 82 („Gesichtsfelderkennung").

für den Einsatz automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger erfüllen muss. Insbesondere ist der Zweck des maschinellen Datenabgleichs („zur Aufklärung einer Straftat oder zur Ermittlung des Aufenthaltsortes einer Person") im Hinblick auf die Eingriffsintensität automatisierter Gesichtserkennung zu unbestimmt formuliert, die Art der Datenabfrage bzw. das technische Eingriffsinstrument (Gesichtserkennung) sind nicht näher spezifiziert, die zum Abgleich zugelassenen Datenbanken sind nicht hinreichend begrenzt und die Verwendung höchstpersönlicher biometrischer Merkmale geht nicht aus der Norm hervor.

Diese Bedenken hinsichtlich der Bestimmtheit und Normenklarheit können auch nicht dadurch entkräftet werden, dass einige der Defizite durch Auslegung zu beseitigen wären. Eine solche Auslegung ist bei Bestimmtheitsmängeln nur mit Rücksicht auf den Sinn und Zweck des Bestimmtheitsgrundsatzes möglich.[834] Sie kommt aber jedenfalls, so das Bundesverfassungsgericht, dann „nicht in Betracht, wenn es an einem die wesentlichen Fragen umfassenden Regelungskern fehlt, der auf einen erklärten objektivierten Willen des Gesetzgebers zurückgeführt werden kann".[835] Denn wenn bei einer Vorschrift, die aus sich heraus weder bestimmte Ausschlusstatbestände enthält, noch deutlich den Zweck der Regelung erkennen lässt, eine verfassungskonforme Auslegung gleichwohl zulässig wäre, dann liefe der Gesetzesvorbehalt leer, der Eingriffe in ein Grundrecht einer gesetzlichen Regelung zuweist und den Gesetzgeber verpflichtet, Art und Umfang des Eingriffs selbst festzulegen.[836]

Die Vorschrift des § 98c StPO genügt daher auch mit Blick auf das Gebot der Bestimmtheit und Normenklarheit nicht den Anforderungen, die an eine Ermächtigung für den Einsatz automatisierter Gesichtserkennung zu stellen sind. Der Einsatz automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger kann daher – entgegen der bisherigen allgemeinen Auffassung in Praxis und Literatur[837] – *nicht* auf § 98c StPO gestützt werden.

834 BVerfGE 120, 378 (423).
835 BVerfGE 120, 378 (423).
836 BVerfGE 120, 378 (423 f.).
837 Soweit § 98c StPO als taugliche Rechtsgrundlage für den Einsatz automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger angesehen wird, beruht dies darauf, dass von einem nur „vergleichsweise geringen" Eingriffsgewicht ausgegangen wird, so *Schindler*, Biometrische Videoüberwachung, 2021, 548; *Hornung/Schindler*, ZD 2017, 203, 207; dem zustimmend BeckOK StPO/*Gerhold*, 49.

II. Sonstige Rechtsgrundlagen

Im Folgenden werden weitere Vorschriften beleuchtet, die als Rechtsgrundlagen für die Verwendung von Gesichtserkennungssoftware zu Identifizierung unbekannter Verdächtiger in Betracht kommen.

1. § 98a, b StPO

Bei der Rasterfahndung (§§ 98a, b StPO) werden die Möglichkeiten der elektronischen Datenverarbeitung genutzt, um Nichtverdächtige auszuschließen oder Personen festzustellen, die weitere für die Ermittlungen bedeutsame Prüfungsmerkmale erfüllen.[838] Während es bei § 98c StPO um den Abgleich mit Daten geht, die bereits bei den Strafverfolgungsbehörden vorhanden sind, betrifft die Rasterfahndung den Abgleich mit bei anderen Stellen gespeicherten Daten. Hierfür sondert die speichernde (öffentliche oder nicht öffentliche) Stelle die für den Abgleich erforderlichen Daten aus den Datenbeständen aus und übermittelt sie den Strafverfolgungsbehörden (§ 98a Abs. 2 StPO).[839] Diese Daten werden dann anhand von Prüfungsmerkmalen (z. B. „männlich, Alter 18 bis 40 Jahre, Student oder ehemaliger Student, islamische Religionszugehörigkeit, Geburtsland oder Nationalität bestimmter, im Einzelnen benannter Länder mit überwiegend islamischer Bevölkerung“[840]) durchsucht; dabei werden im Regelfall in mehreren Schritten verschiedene Datensätze abgeglichen.[841] Bei der positiven Rasterfahndung werden Personen herausgefiltert, die als Schnittmenge diese Prüfungsmerkmale erfüllen; bei der negativen Rasterfahndung werden Personen ausgeschieden, bei denen die Prüfungsmerkmale nicht

---

Ed., Stand: 1.10.2023, StPO § 98c Rn. 1 und *Bauer/Gogoll/Zuber*, Gesichtserkennung, 2021, 51; vgl. auch *Petri*, GSZ 2018, 144, 146.

838 Näher zur Rasterfahndung etwa *Eckstein*, Ermittlungen zu Lasten Dritter, 2013, 280 ff.

839 Hingegen handelt es sich nicht um eine Rasterfahndung, wenn die Strafverfolgungsbehörden einzelne Auskünfte erhalten (also nicht die Gesamtdateien zum weiteren Abgleich mit anderen Dateien); vgl. BVerfG, NJW 2009, 1405, 1406.

840 So die Suchanfrage für (allerdings präventive) Rasterfahndung nach den Anschlägen vom 11.9.2001, BVerfG, NJW 2006, 1939. Es wurde vermutet, dass sich islamistische Terroristen als sogenannte „Schläfer“ in der Bundesrepublik Deutschland aufhalten sollen.

841 Vgl. MüKoStPO/*Hauschild*, 2. Aufl. 2023, StPO § 98a Rn. 3.

(alle) zutreffen.[842] Der Einsatz von Gesichtserkennung zur Identifizierung unbekannter Verdächtiger hat zwar gewisse Parallelen mit der Rasterfahndung, jedoch werden hier keine Prüfungsmerkmale im Sinne der §§ 98a, b StPO abgeglichen.[843] Auf die Vorschriften zur Rasterfahndung (§§ 98a, b StPO) lässt sich der Einsatz automatisierter Gesichtserkennung daher nicht stützen.

2. § 81b Abs. 1 Alt. 1 StPO

Die Vorschrift des § 81b StPO regelt erkennungsdienstliche Maßnahmen bei dem Beschuldigten und erlaubt unter anderem (Alt. 1), soweit es für die Zwecke der Durchführung des Strafverfahrens notwendig ist, Lichtbilder und Fingerabdrücke des Beschuldigten auch gegen seinen Willen aufzunehmen und Messungen und ähnliche Maßnahmen an ihm vorzunehmen. Die „Aufnahme" von Lichtbildern erfasst aber bereits ihrem Wortlaut nach nicht auch den Abgleich von Lichtbildern. Auch handelt es sich bei dem Einsatz von Gesichtserkennung nicht um „Messungen und ähnliche Maßnahmen".[844] Der Umstand, dass automatisierte Gesichtserkennung ursprünglich auf Messung von Gesichtsmerkmalen basierte, ändert hieran nichts – zumal die heute verwendeten Algorithmen so komplex sind, dass selbst die Entwickler die Rechenschritte nicht nachvollziehen können und ohnehin nicht mehr von einem „Messen von Abständen" gesprochen werden kann. Mit „Messungen" im Sinne des § 81b Abs. 1 Alt. 1 StPO sind manuelle Messungen, etwa von Körpergröße, Gewicht oder Schuhgröße,[845] gemeint. Automatisierte Gesichtserkennung wäre erstens – wenn überhaupt – eine automatisierte Messung und vor allem aber auch ein automatisierter Abgleich zuvor „ausgemessener" Merkmale und daher eine gänzlich andere Maßnahme als eine Messung der Schuhgröße. § 81b Abs. 1 Alt. 1 StPO ist daher ebenfalls keine taugliche Rechtsgrundlage.[846]

842 KK-StPO/*Greven*, 9. Aufl. 2023, StPO § 98a Rn. 2.
843 So auch *Schindler*, Biometrische Videoüberwachung, 2021, 424, der zudem darauf hinweist, dass bei der Recherche mit Gesichtserkennung in polizeilichen Lichtbilddatenbanken keine „externen" Datensätze durchsucht werden.
844 Ebenso auch *Schindler*, Biometrische Videoüberwachung, 2021, 431.
845 Vgl. OVG Magdeburg, NJW 2019, 1827, 1832.
846 *Schindler*, Biometrische Videoüberwachung, 2021, 431.

3. § 100h Abs. 1 S. 1 Nr. 1 StPO

Nach § 100h Abs. 1 S. 1 Nr. 1, Abs. 2 StPO dürfen Bildaufnahmen von dem Beschuldigten außerhalb von Wohnungen auch ohne sein Wissen hergestellt werden. Zwar darf das so generierte Material händisch gesichtet werden; dies lässt sich noch auf die Vorschrift des § 100h StPO oder zumindest auf §§ 161, 163 StPO stützen. Nicht mehr erfasst von einem „Herstellen" ist aber angesichts der Eingriffsintensität der automatisierte Abgleich per Gesichtserkennung.[847]

4. § 163b Abs. 1 S. 1 StPO

Auch auf § 163b Abs. 1 S. 1 StPO kann der Einsatz automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger anhand von Lichtbilddatenbanken nicht gestützt werden. Die Vorschrift erlaubt es, die zur Feststellung der Identität eines Beschuldigten „erforderlichen Maßnahmen" zu treffen. Diese generalklauselartige Formulierung[848] ist aber ersichtlich nicht geeignet, die Eingriffe in das Recht auf informationelle Selbstbestimmung zahlreicher Unbeteiligter in der Datenbank gespeicherter Personen zu legitimieren. § 163b Abs. 1 S. 1 StPO ist daher ebenfalls keine taugliche Rechtsgrundlage für die hier untersuchte Einsatzvariante von Gesichtserkennung.[849]

5. §§ 161, 163 StPO

Aufgrund ihrer Unbestimmtheit können auch die Ermittlungsgeneralklauseln der §§ 161, 163 StPO nicht als Ermächtigung herangezogen werden. Zudem sind wegen der Vorbehaltsklausel („soweit nicht andere gesetzliche Regelungen …") bei speziell geregelten Ermittlungseingriffen die entsprechenden Vorschriften anzuwenden; deren Voraussetzungen dürfen nicht durch die Ermittlungsgeneralklausel umgangen werden.[850] Für einen

847 So im Ergebnis auch *Hornung/Schindler*, DuD 2021, 515, 518; *Schindler*, Biometrische Videoüberwachung, 2021, 420.
848 KK-StPO/*Weingarten*, 9. Aufl. 2023, StPO § 163b Rn. 12.
849 So im Ergebnis auch *Schindler*, Biometrische Videoüberwachung, 2021, 434 f. mit anderer Begründung.
850 MüKoStPO/*Kölbel/Ibold*, 2. Aufl. 2024, StPO § 161 Rn. 7.

justizinternen Datenabgleich wäre § 98c StPO heranzuziehen, der aber bereits den Anforderungen an eine Rechtsgrundlage für den Einsatz automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger nicht genügt.

6. § 48 BDSG

Auch die Vorschrift des § 48 BDSG ist keine taugliche Rechtsgrundlage[851] zur Identifizierung unbekannter Verdächtiger per Gesichtserkennung (und allgemein zur Verarbeitung sensibler Daten). Angesichts ihrer Unbestimmtheit und mangelnden Normenklarheit[852] dürfte sie verfassungswidrig sein, sofern mit ihr eine generelle Rechtsgrundlage zur Verarbeitung der dort genannten besonderen Kategorien von Daten bestehen soll.[853] *Rückert* weist insofern zu Recht darauf hin, dass insbesondere Anlass und Grenzen (bis auf die „unbedingte Erforderlichkeit") der Datenverarbeitung nicht hinreichend konkret festgelegt sind und dass § 48 BDSG nicht einmal einen Anfangsverdacht voraussetzt.[854] Davon abgesehen: Die Vorschrift ist derart generalklauselartig[855] formuliert („Die Verarbeitung besonderer Kategorien personenbezogener Daten ist nur zulässig, wenn sie zur Aufgabenerfüllung unbedingt erforderlich ist."), dass sie jedenfalls für eine eingriffsintensive Maßnahme wie die automatisierte Gesichtserkennung zur Ermittlung der Identität unbekannter Verdächtiger nicht herangezogen werden kann.[856]

---

851 Nach BT-Drs. 18/11325, 111 soll § 48 BDSG eine Rechtsgrundlage sein; siehe auch Gola/Heckmann/*Braun*, 3. Aufl. 2022, BDSG § 48 Rn. 1. Kritisch hierzu Paal/Pauly/*Frenzel*, 3. Aufl. 2021, BDSG § 48 Rn. 4; Sydow/Marsch DS-GVO/BDSG/*Kampert*, 3. Aufl. 2022, BDSG § 48 Rn. 36; siehe auch *Johannes/Weinhold*, Das neue Datenschutzrecht bei Polizei und Justiz, 2018, § 1 BDSG Rn. 149; ebenfalls kritisch und vertiefend zu § 48 BDSG *Arzt*, DÖV 2023, 991, 994 ff.

852 Vgl. auch BeckOK DatenschutzR/*Albers/Schimke*, 46. Ed., Stand: 1.8.2023, BDSG § 48 Rn. 9 („relativ unbestimmt").

853 Siehe auch *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, 2023, 536, 776.

854 *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, 2023, 536.

855 Gola/Heckmann/*Braun*, 3. Aufl. 2022, BDSG § 48 Rn. 1. Für eine größere Offenheit mit Blick auf generalklauselartig formulierte Rechtsgrundlagen zur Datenverarbeitung außerhalb sicherheitsrechtlicher Kontexte plädieren *Marsch/Rademacher*, Die Verwaltung, 2021, 1.

856 Sydow/Marsch DS-GVO/BDSG/*Kampert*, 3. Aufl. 2022, BDSG § 48 Rn. 36 mit dem Hinweis, dass Datenverarbeitungen, für die bislang keine Rechtsgrundlage bestand, auch auf Grundlage von § 48 BDSG nicht zulässig sein dürften. Ablehnend

III. Fazit: Keine Rechtsgrundlage

Für den Einsatz automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger anhand von Lichtbilddatenbanken besteht keine strafprozessuale Ermächtigung. Insbesondere kann eine solche Maßnahme nicht auf § 98c StPO gestützt werden. Die Vorschrift verlangt lediglich einen Anfangsverdacht für (irgend-)eine Straftat und beinhaltet keinerlei prozedurale Schutzmechanismen; vor diesem Hintergrund kann sie nur geringfügige Grundrechtseingriffe legitimieren. Ein auf Basis automatisierter Gesichtserkennung vorgenommener Abgleich von Lichtbildern zur Identifizierung unbekannter Verdächtiger ist jedoch kein geringfügiger, sondern ein erheblicher Grundrechtseingriff. Auch genügt § 98c StPO mit Blick auf die Bestimmtheit und Normenklarheit nicht den verfassungsrechtlichen Anforderungen, die an eine Ermächtigung für den Einsatz automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger zu stellen sind. Der Zweck des maschinellen Datenabgleichs („zur Aufklärung einer Straftat oder zur Ermittlung des Aufenthaltsortes einer Person") ist mit Blick auf das erhebliche Eingriffsgewicht automatisierter Gesichtserkennung zu unbestimmt formuliert, die Art der Datenabfrage bzw. das technische Eingriffsinstrument (Gesichtserkennung) sind nicht näher spezifiziert, die zum Abgleich zugelassenen Datenbanken sind nicht hinreichend begrenzt und die Verwendung höchstpersönlicher biometrischer Merkmale geht nicht aus der Norm hervor.

Wie oben bereits angesprochen, verlangt das Bundesverfassungsgericht mit Blick auf technologische Entwicklungen zwar keine gesetzlichen Formulierungen, die jede Einbeziehung kriminaltechnischer Neuerungen ausschließen. Wegen des schnellen und für den Grundrechtsschutz riskanten informationstechnischen Wandels müsse der Gesetzgeber aber „die technischen Entwicklungen aufmerksam beobachten und bei Fehlentwicklungen

---

zum Rückgriff auf § 48 BDSG für den Einsatz von Gesichtserkennung zur Auswertung umfangreichen Datenmaterials (wie nach den G20-Ausschreitungen) *Martini*, NVwZ-Extra 1-2/2022, 1, 9 f.; *Bauer/Gogoll/Zuber*, Gesichtserkennung, 2021, 49 f.; *Schindler*, Biometrische Videoüberwachung, 2021, 445; *Mysegades*, NVwZ 2020, 852, 854; Gola/Heckmann/*Braun*, 3. Aufl. 2022, BDSG § 48 Rn. 3; zumindest in Betracht gezogen dagegen von VG Hamburg, Urt. v. 23.10.2019, 17 K 203/19, BeckRS 2019, 40195 Rn. 75 ff. Wohl insgesamt gegen § 48 BDSG als Rechtsgrundlage für automatisierte Gesichtserkennung in Gefahrenabwehr und Strafverfolgung *Wörner/Blocher*, in: Miró-Llinares/Duvac/Toader/Santisteban Galazarza, Criminalisation of AI-related offences, International Colloquium, 2024, 213, 215.

hinsichtlich der konkreten Ausfüllung offener Gesetzesbegriffe durch die Strafverfolgungsbehörden und die Strafgerichte notfalls durch ergänzende Rechtssetzung korrigierend eingreifen".[857] Mit Blick auf den Einsatz automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger sollte der Gesetzgeber nun umgehend korrigierend eingreifen.

857 BVerfGE 112, 304 (316 f.); vgl. auch BVerfGE 90, 145 (191).