Studien zum Strafrecht 134

Johanna Hahn

Automatisierte Gesichtserkennung in der Strafverfolgung

Nomos DIKE

Studien zum Strafrecht Band 134

Herausgegeben von

Johanna Hahn

Automatisierte Gesichtserkennung in der Strafverfolgung

Nomos

DIKE

Gedruckt mit freundlicher Unterstützung
des Bundesministeriums des Innern und für Heimat.

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in
der Deutschen Nationalbibliografie; detaillierte bibliografische
Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Zugl.: Leipzig, Univ., Diss., 2024

u.d.T.: Der Einsatz automatisierter Gesichtserkennung in der Strafverfolgung

1. Auflage 2025

Publiziert von
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden
www.nomos.de

Gesamtherstellung:
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden

ISBN 978-3-7560-2294-6 (Print)
ISBN 978-3-7489-4945-9 (ePDF)

ISBN 978-3-03891-814-1 (Dike Verlag Zürich/St. Gallen)

DOI: https://doi.org/10.5771/9783748949459

Onlineversion
Nomos eLibrary

Vorwort

Die vorliegende Arbeit wurde im Wintersemester 2023/24 von der Juristenfakultät der Universität Leipzig als Dissertation angenommen. Literatur und Rechtsprechung sind grundsätzlich auf dem Stand vom 31.1.2024. Die Vorgaben der im Juli 2024 veröffentlichten KI-Verordnung der Europäischen Union und einige Beiträge hierzu konnten noch für die Veröffentlichung berücksichtigt werden.

Besonderer Dank gilt an erster Stelle meiner Doktormutter Professorin Elisa Hoven. Sie hat von Anfang an Vertrauen in mich gesetzt, mir große wissenschaftliche Freiheit gelassen und mich immer bei all meinen Vorhaben ganz außergewöhnlich unterstützt. Professor Eric Hilgendorf bin ich zutiefst dankbar für die zügige Erstellung des Zweitgutachtens, seinen fachlichen Rat und für seine Unterstützung meines wissenschaftlichen Wegs.

Die Idee für diese Arbeit stammt aus meiner Station am Bundesministerium der Justiz im Referat RB3 Strafverfahren (Ermittlungsverfahren, Zwangsmaßnahmen) Anfang 2021 unter der Leitung von OStAin BGH Dr. Monika Becker. Als ich mich dort erstmals vertieft mit biometrischer Fernidentifizierung befasste, hat mich dieses Thema gepackt und nicht mehr losgelassen. Professor Eric Hilgendorf und Professor Martin Asholt danke ich dafür, dass sie mit ihren Gutachten für die Studienstiftung des deutschen Volkes bereits zu Beginn Vertrauen in dieses Vorhaben gesetzt haben. Professor Christian Rückert bin ich von Herzen dankbar für den kontinuierlichen Austausch und seine richtungsweisenden Ratschläge an mehreren Stellen des Schreibprozesses. Juniorprofessorin Lucia Sommerer hat mich während der gesamten Promotionszeit durch ihren Rat unterstützt und dadurch maßgeblich zum Gelingen dieser Arbeit beitragen. Professor Hans Kudlich danke ich dafür, dass er mich so herzlich als Habilitandin an seinem Lehrstuhl und im DFG-Graduiertenkolleg „Cyberkriminalität und Forensische Informatik“ aufgenommen hat und mir ermöglicht, meine Forschung zu Strafrecht und neuen Technologien nun auszubauen. Ganz besonders bin ich Professor Jens Bülte dankbar, der mich seit unserem ersten Gespräch zum Tierschutzstrafrecht immer in allen Lebenslagen unterstützt.

Viele der Gedanken in dieser Arbeit stammen aus meiner Zeit an der Harvard Law School. Besonders bereichert haben mich dort die Gespräche

über meine Doktorarbeit mit Professor Christopher Bavitz, Professor James Waldo, Professor Alex Whiting, Professor Jonathan Zittrain und Shira Gur-Arieh. Das Feedback in der Law & Tech Policy Writing Group hat mich ebenso weitergebracht wie der Austausch im Harvard Student Leaders in AI Program am Berkman Klein Center for Internet & Society.

Zutiefst dankbar bin ich auch für die vielen Gespräche über technische Fragen der automatisierten Gesichtserkennung mit Dr. Oren Amsalem (Harvard Medical School), Mathias Ibsen (TU Darmstadt) und vor allem Dr. Martin Knoche (TU München). Unvergleichlich wertvolle Einblicke in die Praxis der Strafverfolgung mit automatisierter Gesichtserkennung ermöglicht haben mir Kay-Uwe Brandt und sein Team (Bundespolizei, Referat 33 – Gesichtserkennung). Die interessanten und kontroversen Diskussionen mit Patrick Rolfes (BKA, Referat ZI 21 – Strategie und Innovation Biometrie) haben mich ebenfalls sehr bereichert. Dr. Lena Leffer danke ich für den fachlichen und persönlichen Austausch über die gesamte Promotionszeit hinweg. Die ideelle und finanzielle Unterstützung der Studienstiftung des deutschen Volkes und der Fulbright Kommission haben dieses Vorhaben enorm erleichtert und mir die nötige Freiheit gegeben. Dem Bundesministerium des Innern und für Heimat danke ich für den gewährten Druckkostenzuschuss. Dr. Maximilian Gerhold, Dr. Nicolai Hahn, Bruno Kaufmann und Dr. Annika Obert haben die Arbeit vollständig oder in großen Teil gelesen. Für ihre Zeit und ihr Feedback bin ich sehr dankbar.

Besonderer Dank gilt darüber hinaus meinen Eltern Bruno und Irmtraud Kaufmann und meinem Bruder Sebastian für ihre Unterstützung bei diesem und all meinen Vorhaben. Meinem Mann Nicolai ist diese Arbeit gewidmet.

Inhaltsverzeichnis

Abbildungsverzeichnis

Kapitel I. Grundlagen

„Daten sind Macht."[1]

A. Einführung

In einer Welt, die täglich mit Informationen überflutet wird, sind nicht Daten Macht, sondern die Fähigkeit, sie zu verarbeiten. Allein Smartphones und Überwachungskameras erstellen, speichern und teilen in kürzester Zeit Milliarden Fotos, Videos und Livestreams; an Daten herrscht kein Mangel. Aber niemand kann sie alle durchforsten und Zusammenhänge herstellen – jedenfalls kein Mensch. Automatisierte Gesichtserkennung macht es jedoch mittlerweile möglich, aus den Datenmassen heimlich einen einzelnen Menschen herauszugreifen, ihn zu identifizieren, zu beobachten und zu orten. Die Technologie kann aus Milliarden Fotos und Videos all diejenigen herausfiltern und zusammenführen, in denen die gesuchte Person auftaucht. Dadurch lässt sich eine Menge über diese Person herausfinden: was sie gerade unternimmt und wo sie sich aufhält, was sie letzte Woche getan hat und ob sie vor einem Parteibüro, in einer Moschee oder bei Protesten war. Automatisierte Gesichtserkennung macht es aber auch möglich, Straftäter durch Überwachungsvideos oder Handyfotos zu identifizieren und Gewalttäter auf der Flucht aufzuspüren und festzunehmen.

Der Einsatz automatisierter Gesichtserkennung in der Strafverfolgung steht nicht in einer dystopischen Zukunft bevor, sondern ist weltweit bereits in vollem Gange. Vor allem in China und Russland ist die Technologie verbreitet.[2] In den USA setzt mindestens jede vierte Polizeibehörde Gesichtserkennung ein;[3] die Hälfte der erwachsenen US-Amerikaner – über

1 Häufige Abwandlung des Ausspruchs „Wissen ist Macht" („nam scientia potestas est") von Francis Bacon, *Bacon*, in: Spedding/Ellis/Heath, The Works of Francis Bacon Vol. XIV, Bd. XIV, 1863, 59, 79.

2 Hierzu Kapitel I. G. II. 1. a) und b).

3 *Garvie/Bedoya/Frankle*, The Perpetual Line-Up: Unregulated Police Face Recognition in America, Center on Privacy & Technology, Georgetown Law, 2016, https://perma.cc/BSF9-9A9C; seit diesem Report aus 2016 dürften die Zahlen noch erheblich gestiegen sein. Alle in dieser Arbeit zitierten Perma-Links sowie die ihnen zugrunde

117 Millionen Menschen – sind in Gesichtserkennungsdatenbanken gespeichert.[4] Zahlreiche Strafverfolgungsbehörden in EU-Staaten verwenden die Technologie ebenfalls, etwa in Frankreich, Österreich, den Niederlanden, Italien, Ungarn und Griechenland;[5] weitere Staaten wie Estland, Rumänien und Spanien sind dabei, sie zu implementieren.[6]

Auch in Deutschland setzen die Strafverfolgungsbehörden bereits auf Gesichtserkennung. Im Gesichtserkennungssystem (GES) des Bundeskriminalamts (BKA) werden jährlich zehntausende Suchläufe durchgeführt; allein die Bundespolizei hat 2022 auf diese Weise rund 2.800 unbekannte Personen identifiziert.[7] Mit Gesichtserkennung kann nach einem Diebstahl, einer Schlägerei oder einem Drogendeal die Identität eines unbekannten Verdächtigen ermittelt werden; ein einziges Foto kann ausreichen. 6,7 Millionen Porträtaufnahmen zu rund 4,6 Millionen Personen (Stand: 2023) können mit dem Gesichtserkennungssystem des BKA durchleuchtet werden.[8]

Dabei ist die Verwendung der Technologie noch weitgehend unreguliert. Auf EU-Ebene war bei der Aushandlung der KI-Verordnung die biometrische Fernidentifizierung – diese umfasst die Gesichtserkennung – ein wesentlicher Streitpunkt.[9] Diese Verordnung des Unionsgesetzgebers ist weltweit der erste Versuch, Anwendungen Künstlicher Intelligenz (KI) umfassend zu regeln; risikoreiche KI-Systeme sollen streng reguliert, besonders risikoreiche Anwendungen verboten werden. Im Dezember 2023 einigten sich Kommission, Rat und Parlament auf eine Regelung; der finale Verordnungstext wurde im Juli 2024 im Amtsblatt der Europäischen Uni-

liegenden Webseiten wurden, sofern nichts anderes angegeben ist, zuletzt abgerufen am 20.1.2024.

4 *Garvie/Bedoya/Frankle*, The Perpetual Line-Up: Unregulated Police Face Recognition in America, Center on Privacy & Technology, Georgetown Law, 2016, https://perma.cc/BSF9-9A9C.

5 Summary report of the project „Towards the European Level Exchange of Facial Images" (TELEFI) 2021, 39 ff., https://perma.cc/T6NE-GTRV.

6 Summary report of the project „Towards the European Level Exchange of Facial Images" (TELEFI) 2021, 60, 116, 126, https://perma.cc/T6NE-GTRV.

7 BT-Drs. 20/5781, 8. Ausführlich zum Ablauf bei der Verwendung des GES Kapitel I. F. I.; zu den technologischen Hintergründen und der Funktionsweise von Gesichtserkennung Kapitel I. E.

8 BT-Drs. 20/7864, 24; BT-Drs. 20/5781, 7.

9 Siehe hierzu nur *Leisegang*, Netzpolitik.org v. 12.6.2023, https://perma.cc/4PNV-AMZ6.

on veröffentlicht.[10] Am 1. August 2024 trat die KI-Verordnung in Kraft.[11] Die Vorschriften der KI-Verordnung zu biometrischer Fernidentifizierung enthalten aber keine Rechtsgrundlage zum Einsatz biometrischer Fernidentifizierung, sondern setzen eine nationale Regelung voraus. In Deutschland existiert jedoch keine spezielle Rechtsgrundlage für den Einsatz automatisierter Gesichtserkennung in der Strafverfolgung. Deren Ausgestaltung ist eine zentrale Herausforderung der Sicherheitsgesetzgebung[12] in der heutigen Zeit.

B. Ziel und Gang der Untersuchung

Diese Arbeit hat das Ziel, in der Rechtswissenschaft eine Debatte über die Regulierung des Einsatzes automatisierter Gesichtserkennung in der Strafverfolgung anzustoßen. Zudem will sie einen ersten Beitrag zu der Frage leisten, wie die Ausgestaltung einer strafprozessualen Regelung aussehen könnte.

In Kapitel I. wird zunächst dargelegt, wie Gesichtserkennung in technischer Hinsicht funktioniert und wie sie in der Strafverfolgung eingesetzt werden kann. Die Arbeit konzentriert sich auf den Einsatz zur Ermittlung der Identität unbekannter Verdächtiger und zeigt, wie BKA, Bundespolizei, Landeskriminalämter und Landespolizeibehörden zu diesem Zweck Gesichtserkennung bereits gegenwärtig verwenden. Zudem werden Chancen und Risiken der Technologie beleuchtet: Thematisiert werden dabei insbesondere die Gefahr von Fehlidentifizierungen und anschließenden Ermittlungen gegen Unbeteiligte sowie die Auswirkungen auf die Gesellschaft insgesamt. Um diesen Risiken zu begegnen, ist ein Blick über die einzelne Maßnahme hinaus auf das System Gesichtserkennung als Ganzes erforderlich.

---

10 Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz), ABl. L 2024/1689 v. 12.07.2024; im Folgenden: KI-VO. Näher zum KI-Verordnungsentwurf der EU-Kommission mit Blick auf die Regulierung der Verwendung biometrischer Fernidentifizierung in der Strafverfolgung *Hahn*, ZfDR 2023, 142.

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

12 Zum Begriff *Gusy*, KritV 2012, 247.

In Kapitel II. wird herausgearbeitet, welche Anforderungen das Verfassungsrecht an den Einsatz von Gesichtserkennung stellt. Im Zentrum steht das verfassungsrichterlich entwickelte Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG). Dabei wird insbesondere untersucht, welche technischen Vorgänge beim Einsatz von Gesichtserkennung zu Grundrechtseingriffen führen und welche Intensität diese Eingriffe haben. Auch wird auf Vorgaben des Primär- und Sekundärrechts der Europäischen Union sowie auf die Europäische Menschenrechtskonvention (EMRK) als regionales Völkerrecht eingegangen. Bei der anschließenden Untersuchung möglicher Rechtsgrundlagen wird überprüft, inwieweit diese den verfassungs- und europarechtlichen Anforderungen genügen.

Kapitel III. analysiert aus kriminologischer Sicht mögliche unbeabsichtigte Folgen und die Darstellung des Einsatzes automatisierter Gesichtserkennung in den Medien. Zunächst wird untersucht, ob und auf welche Weise sich die Verwendung dieser Technologie auf die Selektivität der Strafverfolgung auswirkt. Dabei wird der Frage nachgegangen, welche Delikte und welche Personen in Zukunft stärker verfolgt werden. Anschließend werden mögliche Folgen für Unbeteiligte durch den Einsatz von Gesichtserkennung beleuchtet. Hierfür werden die Fälle der Festnahmen Unschuldiger in den USA nach falschen Gesichtserkennungstreffern ausgewertet und die Ursachen herausgearbeitet. Es wird sowohl auf Fehler der Technologie als auch der Menschen, einschließlich eines Automation bias, eingegangen. Dadurch werden Erkenntnisse darüber gewonnen, wie solche Folgen für Unbeteiligte verhindert werden können. Schließlich wird die Debatte und Wahrnehmung von Gesichtserkennung in den deutschen Medien analysiert. Dabei wird anhand einer qualitativen Inhaltsanalyse von Medienbeiträgen untersucht, welches Bild von der Technologie gezeichnet wird, welche Annahmen dem zugrunde liegen und welche Themen häufig aufgegriffen werden. Dabei wird zum einen herausgearbeitet, welche Bedenken in der medialen Debatte im Vordergrund stehen. Zum anderen wird gezeigt, dass die menschliche Verantwortung für Fehler im Zusammenhang mit Festnahmen nach Gesichtserkennungstreffern regelmäßig verkannt wird. Für das Phänomen, dass der Automation bias in einem zweiten Schritt von den Medien übersehen wird, schlägt diese Arbeit den Begriff des *sekundären* Automation bias vor.

In Kapitel IV. werden ein Vorschlag für die Ausgestaltung der Rechtsgrundlage und weitere konkrete Empfehlungen für eine Regulierung erarbeitet. Hierfür werden die Anforderungen des Verfassungsrechts und des

europäischen Rechts zugrunde gelegt und die Erkenntnisse aus der kriminologischen Untersuchung herangezogen.

C. Gesichtserkennung in der Strafverfolgung: Abgrenzung und Einsatzszenarien

Die automatisierte Gesichtserkennung ist eine Technologie zum Abgleich von Bildern, um Übereinstimmungen zu finden.[13] Sie vergleicht zwei oder mehr Bilder, um zu bestimmen, ob hierauf dieselbe Person gezeigt wird. Vorab wird eine Gesichtserkennungssoftware in der Regel an Fotos von Millionen von Menschen trainiert, bis sie lernt, worauf sie in einem Bild achten muss, um ein Gesicht einem anderen zuzuordnen.

I. Abgrenzung

1. Andere Methoden der biometrischen Erkennung

Neben der automatisierten Gesichtserkennung gibt es noch andere Methoden der biometrischen Erkennung. Biometrische Erkennung ist die automatisierte Erkennung von Menschen anhand biologischer oder verhaltensbezogener Merkmale,[14] etwa anhand von Gesicht, Iris, Retina, Stimme, Fingerabdruck oder Gang. Für die Strafverfolgung besonders interessant sind Methoden, die es ermöglichen, Menschen aus der Ferne zu identifizieren (biometrische Fernidentifizierung), wie etwa die Gesichtserkennung, aber auch die Gangerkennung. Diese Arbeit konzentriert sich auf die automatisierte Gesichtserkennung; andere Methoden der biometrischen Erkennung werden ausgeklammert. Eine gemeinsame Betrachtung aller Methoden der Fernidentifizierung, wie sie etwa die KI-Verordnung[15] auf EU-Ebene vornimmt, erscheint wenig sinnvoll. Zum einen stellen sich bei der Gesichtserkennung andere Probleme als etwa bei der Gangerkennung; insbesondere

13 Ausführlich zum technologischen Hintergrund Kapitel I. E.

14 *Ross/Jain*, in: Jain/Flynn/Ross, Handbook of Biometrics, 2008, 1: „Biometrics is the science of establishing identity of individuals based on their biological and behavioural characteristics." Zu verschiedenen Begriffsbestimmungen, die im Ergebnis aber auf dasselbe hinauslaufen, siehe auch *Schindler*, Biometrische Videoüberwachung, 2021, 123 Fn. 519.

15 Vgl. Art. 3 Nr. 41 KI-VO.

sind Gesichtsbilder – anders als Gangprofile – deutlich leichter zu erfassen und zudem bereits jetzt in großem Umfang in staatlichen Datenbanken gespeichert. Zum anderen ist es kaum möglich, klar abzugrenzen, welche Methoden solche der Fernidentifizierung sind und welche nicht. Wenig eindeutig ist etwa bei einer Erkennung anhand der Iris, ob und wann diese „aus der Ferne" erfolgt. Iriserkennungen waren ursprünglich nur aus einer Entfernung von weniger als einem Meter und mit Kooperation des Betroffenen zuverlässig technisch möglich; in den letzten Jahren wird aber vermehrt daran geforscht, eine höhere Genauigkeit auch für die Erkennung aus mehreren Metern Entfernung und/oder in nicht kontrollierten Settings (unconstrained environments) zu erreichen, bei denen die Betroffenen sich bewegen oder nicht direkt in die Kamera blicken.[16] Wäre Iriserkennung dann derzeit (überwiegend) keine Fernidentifizierung im Sinne der KI-Verordnung, sobald dann eine Erkennung aus größerer Entfernung zuverlässig möglich ist, aber auf einmal doch?[17] Die Methoden der Fernidentifizierung sollten deshalb jeweils separat untersucht werden, sodass sich diese Arbeit auf die Gesichtserkennung konzentriert.

2. Andere Formen der Gesichtsanalyse

Gesichtserkennung ist abzugrenzen von anderen Formen der Gesichtsanalyse wie etwa der automatisierten Erkennung von Emotionen (Emotion recognition),[18] Geschlecht (Gender recognition) und Alter (Age recognition). Diese analysieren zwar auch das Gesicht, haben jedoch, anders als die Gesichtserkennung, nicht das Ziel, die Identität einer Person zu identifizie-

16 Siehe nur *Nguyen/Fookes/Jillela/Sridharan/Ross*, Pattern Recognition 2017, 123; *Tistarelli/Champod* in: Tistarelli/Champod, Handbook of Biometrics for Forensic Science, 2017, 1, 4.

17 Unklar wäre aber, ab welcher Entfernung man von „Fernidentifizierung" per Iriserkennung sprechen könnte, wer diese festlegen soll, wie zuverlässig die Erkennung sein muss und ob es nur auf die Entfernung ankommt oder auch darauf, ob das System zuverlässig erkennt, selbst wenn die betroffenen Personen sich bewegen oder nicht direkt in die Kamera schauen. Zum Ganzen bereits *Hahn,* ZfDR 2023, 142, 153 f.

18 Büro für Technikfolgenabschätzung beim Deutschen Bundestag, Emotionserkennung mittels künstlicher Intelligenz – Perspektiven und Grenzen von Technologien zur Analyse von Gesichtsbewegungen, Themenkurzprofil Nr. 48, https://perma.cc/47GA-RJN2.

ren oder zu verifizieren. Die KI-Verordnung auf EU-Ebene enthält auch Regelungen für Emotionserkennungssysteme.[19]

3. Andere Einsatzbereiche

Automatisierte Gesichtserkennung kann in der Strafverfolgung eingesetzt werden, hat aber auch eine Reihe anderer Anwendungsbereiche. In der Gefahrenabwehr können per Gesichtserkennung beispielsweise gefährliche Personen aufgespürt und von der Begehung einer Straftat abgehalten werden.[20] Im Strafvollzug kann Gesichtserkennung verwendet werden, um die Wege von Inhaftierten innerhalb der Justizvollzugsanstalt zu tracken.[21] An den meisten deutschen Flughäfen können Reisende mit einem Scan ihres elektronischen Reisepasses und einem kurzen Blick in die Kamera die Grenzkontrolle passieren.[22] Auch Private setzen weltweit Gesichtserkennung ein. Supermärkte verwenden automatisierte Gesichtserkennung, um frühere Ladendiebe vom Zutritt abzuhalten.[23] Unternehmen installieren Gesichtserkennung als Zutrittskontrolle für gesicherte Firmengebäude, Stadionbetreiber verwenden die Technologie, um Fans mit einem Stadionverbot zu identifizieren,[24] und viele Smartphone-Besitzer entsperren ihr Gerät mit einem kurzen Blick in die Kamera.

II. Einsatzszenarien in der Strafverfolgung

Zur Strafverfolgung kann automatisierte Gesichtserkennung auf unterschiedliche Weise verwendet werden. In der öffentlichen Debatte wird „Gesichtserkennung" jedoch häufig als Auffangbegriff für unterschiedliche Anwendungen verwendet, deren Ausgangslage, Möglichkeiten und Risiken jeweils ganz andere sind. Es macht einen Unterschied, ob Gesichtserken-

19 Siehe die Definition in Art. 3 Nr. 39 KI-VO; vgl. auch ErwG 18.
20 In Sachsen wurde Gesichtserkennung etwa zur Verhinderung von Grenzkriminalität eingesetzt, siehe hierzu nur *Martini*, NVwZ-Extra 1-2/2022, 1, 11.
21 *Mohapatra*, The Times of India v. 7.4.2023, https://perma.cc/2724-HEGJ.
22 *Bundespolizei*, Teilautomatisierte Grenzkontrolle (EasyPASS), https://perma.cc/5QWX-9MEM.
23 *Satariano/Hill*, The New York Times v. 28.6.2023, https://perma.cc/9BZB-AZL9; bei ihrem Betreten wird ein Security-Mitarbeiter benachrichtigt.
24 *Poppe*, Deutschlandfunk v. 18.8.2019, https://perma.cc/ZQ9X-CE8D.

nung verwendet wird, um den Namen einer Mordverdächtigen anhand einer überschaubaren erkennungsdienstlichen Datenbank zu ermitteln oder um alle Videoaufnahmen einer großen Stadt nach einem Taschendieb zu scannen. Abstrakt über „die Gesichtserkennung" zu diskutieren ist dabei wenig hilfreich; jeder Anwendungsfall muss eigenständig betrachtet werden[25]. Diese unterscheiden sich nicht durch die verwendete Technologie, sondern durch den *Anlass* und den *Zweck*, für den Gesichtserkennung eingesetzt wird.[26] Im Folgenden werden einige Einsatzszenarien näher erläutert.[27]

1. Identitätsermittlung

Automatisierte Gesichtserkennung kann insbesondere dazu verwendet werden, um die Identität von unbekannten Verdächtigen zu ermitteln.[28] Durch die steigende Anzahl an Überwachungskameras und Smartphones werden immer mehr Straftaten auf Video oder Fotos aufgezeichnet – mit dem Gesicht des Täters.[29] In vielen Fällen wird er zumindest beim Betreten oder Verlassen des Tatorts von einer Kamera gefilmt oder von Zeugen oder dem Geschädigten fotografiert. Der unbekannte Verdächtige kann dann identifiziert werden, indem sein Gesicht mit den Bildern in einer Datenbank abgeglichen wird. Dabei könnten die Behörden etwa Führerscheinfotos, Fahndungsbilder oder Lichtbilder in einer erkennungsdienstlichen Datenbank durchsuchen, aber auch die Datenbanken privater Dienstleister wie

25 So zu Recht bereits 2019 die französische Datenschutzbehörde *CNIL*, Reconnaissance faciale: pour un débat à la hauteur des enjeux, 2019, 5, https://perma.cc/37CZ-M5SB („Dans ce contexte, un raisonnement cas d'usage par cas d'usage s'impose."). Zur *CNIL* umfassend *Gerhold*, DuD 2018, 368.

26 Zu verschiedenen Szenarien auch bereits *Hahn*, ZfDR 2023, 142, 147 ff.; zu anderen Klassifizierungen siehe etwa *Schindler*, Biometrische Videoüberwachung, 2021, 189 ff.; *Ferguson*, Minnesota Law Review 2021, 1105, 1114; *Galterio/Shavit/Hayajneh*, A Review of Facial Biometrics Security for Smart Devices, Computers 2018, 37.

27 Weitere Anwendungsfälle sind ebenfalls denkbar, siehe etwa zur Verwendung von Softbiometrie *Schindler*, Biometrische Videoüberwachung, 216 ff.

28 Zu diesem Szenario auch bereits etwa *Klontz/Jain*, A case study on unconstrained facial recognition using the Boston marathon bombings suspects, Technical Report MSU-CSE-13-4, 2013; siehe auch *Ferguson*, Minnesota Law Review 2021, 1105, 1119 ff.; *Schindler*, Biometrische Videoüberwachung, 2021, 201 ff.; *Hornung/Schindler*, ZD 2017, 203, 207; kurz erwähnt auch bei *Petri*, GSZ 2018, 144, 148.

29 Siehe nur Webseite des Bundeskriminalamts, Gesichtserkennung, https://perma.cc/NZ3K-B555.

Clearview AI. Das Unternehmen *Clearview AI* hat von öffentlichen Webseiten wie Facebook, Instagram, Twitter und YouTube Milliarden von Fotos mit Gesichtern zusammengetragen und in einer per Gesichtserkennung durchsuchbaren Datenbank gespeichert.[30] Die Polizei und andere Behörden können kostenpflichtig Zugang zu der App von *Clearview AI* erlangen.

Der zum Abgleich herangezogenen Datenbank kommt eine entscheidende Rolle zu: Ihr Umfang und Inhalt entscheidet darüber, wie viele Gesichter durchleuchtet und wie viele Personen der Gefahr einer fälschlichen Identifizierung ausgesetzt werden.[31] Wenn etwa so große Datenbestände wie die von *Clearview AI* oder eine Datenbank mit Führerscheinfotos gescannt werden, könnte potenziell jede Person identifiziert, aber auch fälschlicherweise als Tatverdächtiger fehlidentifiziert werden. Das Einsatzszenario der Identitätsermittlung ist das weltweit am meisten verbreitete[32] und auch in Deutschland bereits Realität (hierzu noch ausführlich Kapitel I. F.).

2. Auswertung von umfangreichem Datenmaterial

Gesichtserkennung kann die Polizei auch bei der Auswertung von umfangreichem Datenmaterial unterstützen. Nach den Ausschreitungen im Zusammenhang mit dem G20-Gipfel in Hamburg 2017 stellte die Polizei beispielsweise eine umfangreiche Bilddatei zusammen, um diese mittels Gesichtserkennung auszuwerten.[33] Das Material umfasste eigene Aufnahmen der Polizei, Bild- und Videomaterial Privater sowie Aufnahmen der Videoüberwachung von acht verschiedenen S-Bahn-Stationen über einen Zeitraum von fünf Tagen rund um den G20-Gipfel.[34] Aus dieser Grunddatei gewann die Polizei per Gesichtserkennungssoftware eine Referenzdatenbank mit digitalen Darstellungen (sog. Templates[35]) der auf diesen Aufnahmen befindlichen Gesichter. Die Gesichtsbilder Tatverdächtiger wurden

30 *Hill*, The New York Times v. 18.1.2020, https://perma.cc/C4H9-NC6H.

31 Vgl. auch *Schindler*, Biometrische Videoüberwachung, 2021, 191.

32 Siehe etwa für die EU-Staaten Summary report of the project „Towards the European Level Exchange of Facial Images" (TELEFI), 2021, 10 ff., https://perma.cc/T6NE-GTRV.

33 Näher beschrieben bei VG Hamburg Urt. v. 23.10.2019, 17 K 203/19, BeckRS 2019, 40195 Rn. 1 ff.; kritisch zu der Entscheidung *Mysegades*, NVwZ 2020, 852.

34 VG Hamburg, Urt. v. 23.10.2019, 17 K 203/19, BeckRS 2019, 40195 Rn. 3.

35 So noch die Formulierung in VG Hamburg, Urt. v. 23.10.2019, 17 K 203/19, BeckRS 2019, 40195 Rn. 4; mittlerweile ist in der computerwissenschaftlichen Literatur der Begriff „Embedding" geläufiger.

dann mit diesen Dateien abgeglichen, um herauszufinden, wo diese Personen erneut auftauchten. Hierdurch konnten weitere Erkenntnisse über diese Verdächtigen gewonnen werden, etwa zu ihrem Vor- und Nachtatverhalten oder weiteren Straftaten. Die Referenzdatenbank vernetzte die Polizei nicht mit anderen Dateien oder Erkenntnisquellen, sodass die Unbeteiligten nicht namentlich identifiziert werden konnten.

3. Digitale Beobachtung

Gesichtserkennung ermöglicht es der Polizei auch, einen Verdächtigen auf Videoaufnahmen zu beobachten, anstatt ihm physisch zu folgen.[36] In Städten, die mit einem Netzwerk an Überwachungskameras ausgestattet sind, kann eine Person so auf Schritt und Tritt aus der Ferne digital verfolgt werden. Die Beobachtung ist in Echtzeit möglich, Gesichtserkennungssoftware kann aber auch Video- und Fotomaterial aus der Vergangenheit durchsuchen und dabei das Gesicht des Verdächtigen aus einer Reihe von gespeicherten Aufzeichnungen aus der Vergangenheit herausfiltern und darin tracken. Als Datenmaterial kommen etwa Aufnahmen von öffentlichen Plätzen, Flughäfen und Bahnhöfen in Betracht, aber ebenso Fotos und Videos, die Private zur Verfügung stellen. Die Beobachtung erfolgt mit dem Ziel, mehr Informationen zu gewinnen, also zum Beispiel herauszufinden, welche Orte der Verdächtige[37] häufig aufsucht[38] oder mit wem er regelmäßig interagiert. Dadurch können Mittäter aufgespürt oder weitere Ermittlungsansätze generiert werden. Dieses Einsatzszenario ähnelt dem soeben besprochenen; bei der Auswertung von umfangreichem Datenmaterial steht jedoch ein konkretes komplexes *Deliktsgeschehen* mit vielen unterschiedlichen Szenen und Beteiligten im Vordergrund; die zahlreichen Videoaufnahmen und Fotos sollen durch Gesichtserkennung bewältigbar gemacht werden. Bei der digitalen Beobachtung ist Ausgangspunkt dagegen der Verdacht gegen eine *Person*. In Deutschland wird Gesichtserkennung auf diese Weise jedoch noch nicht eingesetzt.

---

36 *Ferguson*, Minnesota Law Review 2021, 1105, 1122 f.; *Garvie/Moy*, America Under Watch: Face Surveillance in the United States, Center on Privacy & Technology, Georgetown Law, 2019, https://perma.cc/5A5T-DHYJ.

37 Auch können Nichtverdächtige beobachtet werden, beispielsweise um den Aufenthaltsort eines Verdächtigen zu ermitteln.

38 Dies gilt nicht nur für Bilder, bei denen der Ort sichtbar 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.

4. Echtzeit-Fahndung

Mit automatisierter Gesichtserkennung kann auch der aktuelle Aufenthaltsort einer Person ermittelt werden. Insbesondere kann das Gesicht einer Person in Echtzeit lokalisiert werden, um sie festzunehmen, etwa wenn sie eines Gewaltverbrechens verdächtig ist oder sich auf der Flucht befindet.[39] Hierzu scannt Gesichtserkennungssoftware in Echtzeit Videomaterial von öffentlichen Plätzen, Flughäfen und Bahnhöfen und gleicht die Gesichter der Passanten mit denen von gesuchten Personen auf einer Fahndungsliste („Watchlist") ab.[40] Sobald das Gesicht eines Gesuchten erkannt wird, löst das System einen Alarm aus. Die darüber informierten Polizisten entscheiden dann, ob sie den Betroffenen anhalten, seinen Ausweis verlangen oder ihn festnehmen.

Diese Form der Echtzeit-Gesichtserkennung wird in Deutschland nicht eingesetzt,[41] sie wurde jedoch in der Vergangenheit erprobt. Zuletzt testete die Bundespolizei in den Jahren 2017 und 2018 biometrische Gesichtserkennung am Bahnhof Berlin Südkreuz zur Unterstützung polizeilicher Fahndung.[42] Das Projekt wurde stark kritisiert[43] und die Erkennungssysteme, soweit bekannt, nach der Testphase nicht eingesetzt. Sachsen war das einzige Bundesland, das Echtzeit-Gesichtserkennung von Sommer 2019 bis Dezember 2023 zuließ.[44] Auf öffentlichen Straßen im Grenzgebiet durfte der Polizeivollzugsdienst Bildaufnahmen machen und personenbezogene

39 Zu diesem Szenario näher *Schindler*, Biometrische Videoüberwachung, 2021, 190 ff.; siehe auch *Martini*, NVwZ-Extra 1-2/2022, 1, 8 ff.; *Hornung/Schindler*, ZD 2017, 203, 207 f.; kurz erwähnt bei *Petri*, GSZ 2018, 144, 147.

40 *Ferguson*, Minnesota Law Review 2021, 1105, 1123 f.; *Li/Jain*, in: Li/Jain, Handbook of Face Recognition, 2011, 1, 3, 12.

41 Summary report of the project „Towards the European Level Exchange of Facial Images" (TELEFI) 2021, 11, https://perma.cc/T6NE-GTRV.

42 *Bundespolizei*, Teilprojekt 1 „Biometrische Gesichtserkennung" des Bundespolizeipräsidiums im Rahmen der Erprobung von Systemen zur intelligenten Videoanalyse durch das Bundesministerium des Innern, für Bau und Heimat, das Bundespolizeipräsidium, das Bundeskriminalamt und die Deutsche Bahn AG am Bahnhof Berlin Südkreuz im Zeitraum vom 01.08.2017 – 31.07.2018, 2018.

43 Siehe etwa der *Chaos Computer Club*, Pressemitteilung vom 13.10.2018, https://perma.cc/45BE-3SX5. Anders dagegen *Bundesministerium des Innern und für Heimat*, Pressemitteilung v. 11.10.2018, https://perma.cc/Z7YV-9C22 (die Systeme hätten sich „bewährt").

44 Rechtsgrundlage war § 59 des Sächsischen Polizeivollzugsdienstgesetz (SächsPVDG). Die Vorschrift trat gem. § 108 Abs. 1 SächsPVDG am 31. Dezember 2023 außer Kraft.

Daten, auch per Gesichtserkennung in Echtzeit,[45] abgleichen.[46] Nach einer Evaluierung wurde die zunächst auf drei Jahre befristete Befugnis nicht verlängert; das sächsische Innenministerium erklärte, der „technische und personelle Aufwand" sei zu groß, auch habe sich „der fachliche Erfolg im Praxisbetrieb nicht eingestellt".[47] Eine Verlängerung der Befugnisnorm sei damit nicht verhältnismäßig.

D. Forschungszuschnitt dieser Arbeit

Diese Arbeit beleuchtet den Einsatz automatisierter Gesichtserkennung in der Strafverfolgung zur Ermittlung der Identität unbekannter Verdächtiger aus rechtlicher und kriminologischer Perspektive. Auf dieser Basis werden konkrete Vorschläge für eine Regulierung erarbeitet. Die Gründe für diesen Zuschnitt der Arbeit sind das besondere Gefährdungspotenzial der Gesichtserkennung im Allgemeinen (I.) und die Relevanz des Einsatzszenarios der Identitätsermittlung im Besonderen (II.) sowie der Umstand, dass eine Forschungslücke besteht (III.) mit Blick auf das Erfordernis einer Regulierung (IV.).

I. Besonderes Gefährdungspotenzial der Gesichtserkennung

Die Verwendung automatisierter Gesichtserkennung in der Strafverfolgung birgt ein besonderes Gefährdungspotenzial. Das liegt zunächst an dem besonders sensiblen Einsatzbereich der Strafverfolgung. Automatisierte Gesichtserkennung kann in vielen Lebensbereichen eingesetzt werden, in den Händen von Strafverfolgungsbehörden entfaltet die Technologie aber erhöhte Risiken. Wenn Gesichtserkennung beim Zutritt zu einem Firmengebäude fehlschlägt, muss die Zugangskontrolle manuell nachgeholt werden – eine kleine Unannehmlichkeit. Wenn Gesichtserkennung in der Strafverfolgung fehlschlägt, wird gegen den Betroffenen womöglich ermittelt, im schlimmsten Fall kann er – ohne der Täter zu sein – strafprozessualen

45 Dies ergibt sich nicht eindeutig aus dem Wortlaut, siehe aber LT-Drs. SN 6/14791, 186 (Verweis auf biometrische Daten).

46 Zu Recht kritisch zu § 59 SächsPVDG als Rechtsgrundlage *Schindler*, Biometrische Videoüberwachung, 2021, 541 ff., siehe auch *Martini*, NVwZ 2022, 30, 31.

47 *Sächsisches Staatsministerium des Innern*, Pressemitteilung v. 22.8.2023, https://perma.cc/6K7W-CVVN.

Zwangsmaßnahmen wie der Wohnungsdurchsuchung oder der Untersuchungshaft unterliegen oder gar unschuldig verurteilt werden.[48] In den USA wurden bereits mindestens sechs schwarze Menschen unschuldig festgenommen, nachdem ein Gesichtserkennungsalgorithmus sie fälschlicherweise als Straftäter identifiziert hatte.[49]

Aber auch – und gerade – wenn Gesichtserkennung gut funktioniert, kann die Technologie eine Gefahr darstellen, und zwar vor allem dann, wenn mit ihr illegitime Strafverfolgung betrieben wird.[50] Polizeibehörden in China integrieren Gesichtserkennungstechnologie in ihre stetig wachsenden Netze an Überwachungskameras, um so zum Beispiel die ethnische Minderheit der Uiguren digital zu beobachten und Informationen über ihr Kommen und Gehen aufzuzeichnen.[51] In Russland werden Demonstrierende wegen angeblicher Straftaten bei Demonstrationen nicht nur vor Ort festgenommen, sondern noch Tage später zu Hause – identifiziert per Gesichtserkennung.[52]

Das Gefährdungspotenzial der Verwendung automatisierter Gesichtserkennung in der Strafverfolgung geht aber auch über die Risiken hinaus, die jeder Strafverfolgungsmaßnahme und -technologie immanent sind. In dieser Hinsicht markiert der breite Einsatz automatisierter Gesichtserkennung einen Wendepunkt bei der Verwendung neuer Strafverfolgungstechnologien. Das disruptive Potenzial der Technologie beruht auf dem neuartigen Zusammentreffen von fünf Faktoren: Streubreite, Fehleranfälligkeit, Heimlichkeit, Vernetzungsmöglichkeit und Biometrie.

1. Streubreite

Strafprozessuale Ermittlungsmaßnahmen richten sich üblicherweise in erster Linie gegen den Beschuldigten. Er wird körperlich untersucht, seine Post gelesen, seine Wohnung durchsucht. Diese Maßnahmen können zwar vereinzelt auch Dritte treffen: den Verletzten, die Geschäftspartnerin, den Mitbewohner. Unter Umständen kann auch eine große Anzahl Unbeteiligter betroffen sein, etwa bei der Rasterfahndung oder der automatisierten

48 Zu diesem Problem Kapitel I. G. II. 1. a) und 2. a) sowie ausführlich Kapitel III. B.
49 Zu diesen Fällen näher unten Kapitel III. B. I. 1.
50 Näher zu den Gefahren (auch) unabhängig von der Fehleranfälligkeit von Gesichtserkennung Kapitel I. G. II. 2. b) und c).
51 *Mozur*, The New York Times v. 14.4.2019, https://perma.cc/85V6-WAML.
52 *Solopov*, Meduza v. 27.4.2021, https://perma.cc/KD8C-BCGJ.

Kfz-Kennzeichenkontrolle. Dazu bedarf es aber einer besonderen Ermächtigungsgrundlage mit engen Voraussetzungen, so etwa § 163g StPO (automatische Kennzeichenerfassung), §§ 98a, b StPO (Rasterfahndung), § 81c StPO (Untersuchung anderer Personen als des Beschuldigten), § 103 StPO (Durchsuchung bei anderen Personen).

Automatisierte Gesichtserkennung trifft nicht vorrangig den Beschuldigten, sondern hauptsächlich Unbeteiligte. Um die Identität eines Verdächtigen anhand einer polizeilichen Datenbank zu ermitteln, müssen alle Bilder der jeweiligen Datenbank durchleuchtet werden.[53] Um einen gesuchten Verdächtigen an einem Bahnhof zu lokalisieren, müssen alle Passantinnen und Passanten per Gesichtserkennung gescannt werden. Und als die Polizei Hamburg zur Aufarbeitung von Straftaten im Zusammenhang mit dem G20-Gipfel Gesichtserkennungssoftware verwendete, durchleuchtete die Technologie in über 95 % der Fälle die Gesichter von verdachtsunabhängig einbezogenen Personen.[54]

2. Fehleranfälligkeit

Auch birgt Gesichtserkennung das Risiko, dass Unschuldige[55] als Verdächtige identifiziert und dann strafprozessualen Ermittlungsmaßnahmen ausgesetzt werden. Diese Gefahr besteht grundsätzlich immer im Ermittlungsverfahren, da sich die Maßnahmen naturgemäß gegen *Verdächtige* (nicht gegen Verurteilte) richten. Gesichtserkennung erhöht aber die Wahrscheinlichkeit, dass Unbeteiligte beschuldigt werden und dass der Fehler wegen

53 Um eine Person über das Gesichtserkennungssystem GES zu finden, müssen alle 6,7 Millionen Porträtaufnahmen zu rund 4,6 Millionen Personen gescannt werden.

54 Nach Angaben der Polizei sind ca. 3.500 Ermittlungsverfahren eingeleitet worden; in der Datenbank waren die Gesichter einer Zahl von Unbeteiligten im sechsstelligen Bereich. Selbst wenn man „nur" 100.000 Unbeteiligte zugrunde legt, wären 96,5 Prozent der in der Datenbank erfassten Personen Unbeteiligte.

55 Zwar ist auch derjenige, der eine Straftat tatsächlich begangen hat, im strafprozessualen Sinne unschuldig, bis er verurteilt wird. Der Begriff „Unschuldiger" soll in dieser Arbeit aber nur Personen erfassen, bei denen sich ex post herausstellt, dass sie die Tat nicht begangen haben. Teilweise wird in dieser Arbeit auch der Begriff „Unbeteiligter" verwendet, um deutlich zu machen, dass es sich meist um Personen handelt, die nicht einmal annähernd etwas mit dem strafrechtlichen Geschehen zu tun hatten.

großer Ähnlichkeit des Aussehens[56] nicht immer erkannt wird.[57] Dabei besteht die Gefahr, dass gänzlich Unbeteiligte in den Fokus der Polizei geraten, die nicht einmal in der Nähe des Tatorts waren oder anderweitig in das Geschehen verwickelt sein könnten: In den USA wurde beispielsweise ein Mann nach einem falschen Gesichtserkennungs-Match verdächtigt, in einem Geschäft in einem Vorort von New Orleans einen Diebstahl begangen zu haben, einem Ort, an dem er noch nie gewesen war – drei Staaten und sieben Stunden Autofahrt entfernt von seiner Heimatstadt.[58] Der einzige Ansatzpunkt, um gegen ihn zu ermitteln, war der Gesichtserkennungstreffer.

3. Heimlichkeit

Mit Gesichtserkennung können die Strafverfolgungsbehörden heimlich aus einer Menge einen einzelnen Menschen herausgreifen, ihn identifizieren, beobachten und orten – ohne dass er dies jemals erfährt. Ob Kameras an Bahnhöfen, Flughäfen und anderen öffentlichen Plätzen hängen, können Bürgerinnen und Bürger meist noch erkennen. Aber sie können nicht wissen, ob diese mit einem Gesichtserkennungssystem verbunden sind. Wer erkennungsdienstlich behandelt wurde, weiß zwar, dass sein Lichtbild bei der Polizei gespeichert ist; wann und wie oft sein Bild automatisiert mit demjenigen unbekannter Verdächtiger abgeglichen wird, weiß er jedoch nicht. Durch die Heimlichkeit ist es kaum oder nicht möglich, den Maßnahmen zu entgehen, präventiv Rechtsschutz zu suchen oder nachzuvollziehen, ob die Strafverfolgungsbehörden alle Vorgaben einhalten (zumal, wenn keine konkreten gesetzlichen Vorgaben bestehen). Das deutsche Strafprozessrecht sieht zwar durchaus vor, dass die Heimlichkeit einer

56 Zwar können als Match auch Personen auftauchen, die ein anderes Geschlecht, eine andere Hautfarbe oder ein ganz anderes Alter als der Gesuchte haben, denn die Technologie vergleicht nur die biometrischen Merkmale (hierzu etwa *Wimmer*, Süddeutsche Zeitung v. 16.1.2016, https://perma.cc/5AWG-M9DZ). Anders wäre dies, wenn zusätzlich nach Geschlecht, Alter usw. gefiltert würde. Die Wahrscheinlichkeit, dass sich Personen mit ähnlichen biologischen Merkmalen auch aus Sicht eines menschlichen Betrachters ähnlich sehen, ist aber hoch. Siehe auch für Fälle, in denen Gesichtserkennungssysteme eine Übereinstimmung sehen, ein Mensch jedoch ohne Probleme erkennt, dass es sich um unterschiedliche Personen handelt *Knoche/Rigoll,* 18th International Conference on Machine Vision and Applications 2023, arXiv, 1, 4.

57 Siehe hierzu die Fälle in Kapitel III. B. I. 1.

58 Siehe hierzu *Hill/Mac*, The New York Times v. 31.3.2023, https://perma.cc/98M2-VMHT sowie Kapitel III. B. I. 1. e).

Maßnahme durch Verfahrensvorgaben (z. B. spätere Benachrichtigung des Betroffenen, siehe auch § 101 Abs. 4 StPO) oder andere Absicherungen (z. B. Berichtspflichten) kompensiert. Solche Vorgaben sind bei der Gesichtserkennung aber gerade mangels ausdrücklicher gesetzlicher Grundlage nicht geregelt.

4. Vernetzungsmöglichkeit

Die Gesichtserkennungssoftware erstellt von jedem Gesicht ein mathematisches Modell (Face embedding), sodass ein automatisierter Abgleich mit anderen Aufnahmen möglich ist, die ebenfalls dateikompatibel gemacht wurden. Durch eine Vernetzung mit einer Personalausweis-, Pass- oder Führerscheindatenbank könnte jede Person innerhalb von Minuten identifiziert werden, durch eine Vernetzung mit Echtzeitdaten aller staatlichen Überwachungskameras in Kürze geortet werden. Bereits heute sind die Lichtbilder von Personalausweis und Reisepass bei der Ausweisbehörde gespeichert (§ 23 Abs. 3 PAuswG; § 21 Abs. 2 PassG).[59] An Flughäfen, Bahnhöfen und öffentlichen Plätzen sind Überwachungskameras bereits vielfach im Einsatz.[60] Zwar ist die automatisierte Vernetzung der Daten derzeit nicht zulässig, siehe zu den Voraussetzungen für einen automatisierten Abruf von Lichtbildern §§ 15, 25 PAuswG, §§ 17, 22a PassG. Das ändert jedoch nichts daran, dass sie faktisch möglich ist und durch Rechtsänderung sofort auch legal möglich wäre.[61]

5. Biometrie

Auch die automatisierte Kennzeichenzeichenerfassung und die (aufgrund der Unionsrechtswidrigkeit ausgesetzte) Vorratsdatenspeicherung treffen eine Vielzahl Unbeteiligter, erfolgen heimlich und bergen die Gefahr der

59 Die Errichtung einer bundesweiten Datenbank biometrischer Merkmale ist jedoch (wenn auch nur einfachgesetzlich) untersagt, vgl. § 26 Abs. 4 PAuswG, § 4 Abs. 3 S. 2 PassG.

60 Schätzungen zufolge existierten Hunderttausende von Überwachungskameras in Deutschland, vgl. *Scholz*, in: Simitis, Bundesdatenschutzgesetz, 8. Aufl. 2014, § 6b Rn. 7 ff.

61 Zu der Gefährdung durch Vernetzungsmöglichkeiten etwa BVerfGE 120, 274, 304 ff. und ausführlich unter Kapitel II. A. I. 2. b) ee).

Vernetzung. Die automatisierte Gesichtserkennung geht in ihrem disruptiven Potenzial noch darüber hinaus, denn sie verwendet Biometrie. 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 (vgl. die Definition in Art. 3 Nr. 13 JI-RL, Art. 4 Nr. 14 DSGVO, § 46 Nr. 12 BDSG und Art. 3 Nr. 34 KI-VO). Dazu gehören etwa DNA und Fingerabdruck einer Person – und die Gesichtsgeometrie.[62] Biometrische Daten sind bei der Gesichtserkennung nicht die Bildaufnahmen selbst, sondern die daraus extrahierten Gesichtsmerkmale. Der Unionsgesetzgeber hat für personenbezogene Daten besonderer Kategorien, zu denen die biometrischen Daten gehören, in Art. 9 Abs. 1, 2 DSGVO und in Art. 10 JI-RL ein besonderes Schutzregime angeordnet. Dabei haben die physischen und physiologischen Merkmale noch eine Besonderheit: Sie sind angeboren und unveränderlich.[63] Wird eine Person einmal in einer Gesichtserkennungsdatenbank gespeichert, kann sie in Zukunft immer wieder identifiziert werden. Das Autokennzeichen lässt sich wechseln, das Gesicht nicht.

6. Fazit

Der Einsatz automatisierter Gesichtserkennung geht mit einem besonderen Gefährdungspotenzial einher, denn er betrifft viele Unbeteiligte (Streubreite), birgt ein spezifisches Fehlerrisiko (Fehleranfälligkeit), erfolgt ohne Wissen der Betroffenen (Heimlichkeit) und ermöglicht die einfache und schnelle Vernetzung verschiedener Informationen (Vernetzungsmög-

62 So auch *Schindler*, Biometrische Videoüberwachung, 2021, 681 f. und *Jandt*, ZRP 2018, 16, 17. Anders (biometrische Daten seien auch die „sog. Rohdaten, also die direkt mit einem Sensor erfassten Merkmale") Kühling/Buchner/*Weichert*, 4. Aufl. 2024, DS-GVO Art. 4 Nr. 14; so auch Taeger/Gabel/*Arning/Rothkegel*, 4. Aufl. 2022, DS-GVO Art. 4 Rn. 398. Bei Gesichtserkennung würde dies bedeuten, dass auch die entsprechenden Lichtbilder biometrische Daten sind, die aber nach ErwG 51 der DSGVO nur dann von der Definition des Begriffes „biometrische Daten" erfasst werden sollen, wenn sie mit speziellen technischen Mitteln verarbeitet werden, die die eindeutige Identifizierung oder Authentifizierung einer natürlichen Person ermöglichen. Siehe auch *Roggenkamp*, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht, § 21 Datenschutz und präventive Tätigkeit der Polizei, 2019, Rn. 61.

63 In gewissem Maße veränderlich sind dagegen verhaltensbasierte biometrische Merkmale wie Unterschrift, Stimme, Bewegung.

lichkeit), die einer Person persönlich und eindeutig zugeordnet werden können (Biometrie). Bislang gibt es in Deutschland keine andere strafprozessuale Maßnahme, die all diese Faktoren vereint und ein solches Gefährdungspotenzial aufweist.

II. Relevantestes Einsatzszenario: Identitätsermittlung

Viele Überlegungen zu Gesichtserkennung lassen sich auf alle Einsatzszenarien übertragen. Aber um ein sinnvolles Regulierungskonzept zu erarbeiten, muss genau nach Anlass, Zweck und spezifischen Risiken der jeweiligen Einsatzvariante differenziert werden. Daher konzentriert sich diese Arbeit auf das für Deutschland relevanteste Szenario mit dem höchsten Risikopotenzial: die Identitätsermittlung. Dieser Einsatz von Gesichtserkennung ist in Deutschland als einziger bereits weit verbreitet,[64] aber nicht ausdrücklich geregelt. Dabei macht ein Blick auf andere Staaten deutlich, welche Risiken hier bestehen.[65]

III. Stand der Forschung und Forschungslücke

Vertieft haben sich bislang nur wenige Beiträge mit dem Einsatz automatisierter Gesichtserkennung in der Strafverfolgung beschäftigt. Die meisten von ihnen befassen sich vorrangig mit der in Deutschland derzeit nicht verwendeten Echtzeit-Gesichtserkennung im öffentlichen Raum als Form intelligenter Videoüberwachung.[66] Der Einsatz automatisierter Gesichtserkennung zur Ermittlung der Identität unbekannter Verdächtiger wird hingegen selten näher betrachtet. Eine Ausnahme bildet *Schindler*, der in seiner 2021 erschienen, nicht spezifisch strafverfahrensrechtlichen Disser-

64 Hierzu Kapitel I. F.

65 Kapitel I. G. II.

66 *Martini*, NVwZ-Extra 1-2/2022, 1; *Kulick*, NVwZ 2020, 1622; *Heldt*, MMR 2019, 285; *Petri*, GSZ 2018, 144. *Martini/Thiessen/Ganter*, Digitale Versammlungsbeobachtung, 2023, 110 ff. befassen sich mit dem Einsatz intelligenter Videoüberwachung (darunter Gesichtserkennung) im Versammlungskontext und gehen dabei auch kurz auf die nachträgliche Gesichtserkennung ein; *Hoffmann* beschäftigt sich vertieft mit dem nichtstaatlichen Einsatz biometrischer Gesichtserkennung, siehe *Hoffmann*, Der nichtstaatliche Einsatz biometrischer Gesichtserkennungssysteme nach der DSGVO, 2023.

tation zur biometrischen Videoüberwachung auf dieses Szenario – neben drei anderen – ebenfalls eingeht und den rechtlichen Rahmen beleuchtet.[67] Er hält es für „noch tragbar", die Verwendung von Gesichtserkennung zur Identitätsermittlung auf bestehende Vorschriften zu stützen[68] und macht daher keine konkreten Vorschläge für eine Regulierung.[69] Eine rechtswissenschaftliche Debatte über die Regulierung findet noch nicht statt.

Über die Darstellung von Gesichtserkennung in der deutschen Medienlandschaft finden sich noch keine kriminologischen oder sozialwissenschaftlichen Untersuchungen. Meist befassen sich die Studien allgemein mit der Einstellung der Bevölkerung zu Überwachungstechnologien.[70] Eine Studie von *Kostka*, *Steinacker* und *Meckel* untersucht die Akzeptanz staatlichen und nichtstaatlichen Einsatzes von Gesichtserkennungstechnologien im öffentlichen Raum, unter anderem in Deutschland.[71] Bei der Frage, welche konkreten Bedenken für die Menschen im Vordergrund stehen, bleibt die Untersuchung allerdings sehr allgemein („privacy violation", „discrimination", „surveillance").[72] In einer Studie aus dem Jahr 2023 gehen sie dem anhand von Online-Befragungen und semi-strukturierten Interviews näher nach; dabei kommen die Forscherinnen zu dem Ergebnis, dass die Akzeptanz von Gesichtserkennung zwischen Bürgern verschiedener Staaten variiert.[73] Insbesondere das Bewusstsein über die Geschichte eines Landes mit staatlicher Überwachung (etwa in der ehemaligen DDR) beeinflusse die Wahrnehmung von staatlicher Gesichtserkennung.[74] Eine nähere kriminologisch-sozialwissenschaftliche Untersuchung der Frage, welche Bedenken beim Einsatz von Gesichtserkennung in der Strafverfolgung im

67 *Schindler*, Biometrische Videoüberwachung, 2021, 283 ff., 312 ff., 422 ff. Da er in seiner rechtlichen Bewertung meist alle vier verschiedenen Einsatzszenarien gemeinsam beleuchtet, kann hier keine genauere Fundstelle angegeben werden.

68 *Schindler*, Biometrische Videoüberwachung, 2021, 548 („Aufgrund des vergleichsweise geringen Eingriffsgewichts sind die bestehenden Vorschriften hinsichtlich ihrer Bestimmtheit aber noch tragbar.").

69 Siehe aber *Schindler*, Biometrische Videoüberwachung, 2021, 548 („Vorzugswürdig sind allerdings Regelungen wie Art. 61 Abs. 2 BayPAG, die die Verwendung biometrischer Erkennung eindeutig benennen. Wünschenswert ist überdies eine stärkere Eingrenzung der für den Abgleich heranzuziehenden Datenbestände in den jeweiligen Vorschriften.").

70 Siehe etwa *van Heek/Arning/Ziefle*, in: Helfert/Klein/Donnelley/Gusikhin, Smart Cities, Green Technologies, and Intelligent Transport Systems, 2017, 170.

71 *Kostka/Steinacker/Meckel*, Public Understanding of Science 2021, 671.

72 *Kostka/Steinacker/Meckel*, Public Understanding of Science 2021, 671, 684.

73 *Kostka/Steinacker/Meckel*, Government Information Quarterly 2023, 1, 5 f.

74 *Kostka/Steinacker/Meckel*, Government Information Quarterly 2023, 1, 6.

Raum stehen, verspricht daher wertvolle Erkenntnisse. Dem dient die in dieser Arbeit durchgeführte qualitative Inhaltsanalyse von Medienbeiträgen (Kapitel III.).

IV. Notwendigkeit einer Regulierung

Der Einsatz automatisierter Gesichtserkennung in der Strafverfolgung ist in Deutschland bereits in vollem Gange, mit jährlich zehntausenden Suchläufen – Tendenz steigend – allein im Gesichtserkennungssystem (GES) des BKA.[75] Die Bundespolizei hat 2022 auf diese Weise rund 2.800 unbekannte Personen identifiziert[76] und auch Landeskriminalämter und Landespolizeibehörden greifen bereits auf die Technologie zurück.[77] Der Einsatz ist gesetzlich nicht ausdrücklich geregelt; stattdessen wird die allgemein gehaltene Vorschrift zum Datenabgleich des § 98c StPO herangezogen. Auch gibt es keine konkreten Vorschläge in der rechtswissenschaftlichen oder rechtspolitischen Debatte dafür, wie eine Regulierung aussehen könnte.

Ausgangspunkt für eine Reglung sind die Anforderungen des Verfassungsrechts, des Unionsrechts und der EMRK. Bei den rechtlichen Mindestvorgaben sollte eine Regulierung aber nicht stehen bleiben, sondern untersuchen, welche zusätzlichen Vorgaben sinnvoll sind. Dabei ist es zum einen wichtig, die Risiken beim Einsatz der Technologie im Blick zu behalten. Wie kann etwa verhindert werden, dass Fehlidentifizierungen dazu führen, dass Unschuldige Ermittlungsmaßnahmen ausgesetzt werden? Zum anderen wäre es klug, die Vorbehalte innerhalb der Bevölkerung besser aufzugreifen. Nach einer im Jahr 2023 durchgeführten repräsentativen Befragung hat über die Hälfte der Deutschen Angst vor KI, vor allem vor einer „flächendeckenden Überwachung".[78] Gerade beim Einsatz neuer Technologien im sensiblen Bereich der Strafverfolgung erscheint es daher angezeigt, die Bedenken näher nachzuvollziehen, aufzugreifen und durch Regulierung zu adressieren. Dadurch könnte auch das Vertrauen der Bevölkerung in

75 Siehe auch Webseite des Bundeskriminalamts, Gesichtserkennung, https://perma.cc/NZ3K-B555 („Aufgrund des steigenden Aufkommens digitaler Aufnahmen, z. B. in den sozialen Netzwerken und der durch Smartphones allzeitigen Möglichkeit Bilder zu fertigen, ist in den nächsten Jahren mit einem weiteren Anstieg der Zahl der GES-Recherchen zu rechnen.").

76 BT-Drs. 20/5781, 8.

77 Kapitel I. F. II.

78 *Fox/Privitera/Reuel*, KIRA Report, 2023, 4.

die Strafverfolgung gestärkt werden. In dieser Arbeit wird daher auch eine qualitative Inhaltsanalyse von Medienbeiträgen durchgeführt und dabei die mediale Debatte über Gesichtserkennung in Deutschland näher untersucht (Kapitel III.), um zu verstehen, welche Bedenken im Vordergrund stehen. Über 70 % der Bevölkerung sind der Ansicht, die Politik unternehme nicht genug gegen mögliche Risiken von KI.[79] Mit Blick auf eine besonders wirkmächtige Strafverfolgungstechnologie besteht für den Gesetzgeber die Möglichkeit, proaktiv diese Bedenken zu adressieren.

Die Verwendung automatisierter Gesichtserkennung zur Ermittlung der Identität unbekannter Verdächtiger muss daher *jetzt* geregelt werden. Es ist weder rechtlich hinnehmbar noch gesellschaftlich vermittelbar, dass eine solche Strafverfolgungstechnologie auf generalklauselartige Vorschriften gestützt und ohne rechtswissenschaftliche und gesellschaftliche Debatte eingesetzt wird. Diese rechtswissenschaftliche Debatte möchte diese Arbeit anstoßen und einen ersten Beitrag hierzu liefern.

E. Technologie

Bevor man sich Gedanken über die rechtliche Einordnung und eine Regulierung von Gesichtserkennung machen kann, müssen die technologischen Grundlagen geklärt werden. Dieser Abschnitt führt zunächst in die grundlegende Unterscheidung zwischen Verifizierung und Identifizierung ein (dazu unter I.) und gibt dann einen Überblick darüber, wie sich die automatisierte Gesichtserkennung entwickelt und in der Strafverfolgung etabliert hat (II.). Anschließend wird dargestellt, wie eine Erkennung anhand von Gesichtserkennung abläuft (III.). Zudem wird vertieft auf die Fehlerraten der Technologie eingegangen (IV.).

I. Verifizierung vs. Identifizierung

Automatisierte Gesichtserkennung kann im Modus der Verifikation (Verifizierung) oder der Identifikation (Identifizierung) betrieben werden.[80] Bei der Verifikation wird eine behauptete Identität überprüft; die biome-

79 *Fox/Privitera/Reuel*, KIRA Report, 2023, 6.

80 Das gilt für alle Methoden der biometrischen Erkennung; speziell zur Gesichtserkennung *Wei/Li*, in: Tistarelli/Champod, Handbook of Biometrics for Forensic Science,

trischen Merkmale der betreffenden Person werden mit nur einem Datensatz abgeglichen (1:1-Abgleich). Das ist etwa der Fall, wenn Gesichtserkennung zum Entsperren des Smartphones oder zur kontaktlosen Bordkartenkontrolle verwendet wird; hier erfolgt jeweils ein Abgleich der (aktuell angefertigten) Bildaufnahme mit dem hinterlegten biometrischen Profil.[81] Hingegen wird bei einer Identifikation die Aufnahme einer Person mit allen Datensätzen in einer Datenbank abgeglichen (1:n-Abgleich), etwa um die Identität eines Verdächtigen anhand von Bildern in einer erkennungsdienstlichen Datenbank zu ermitteln.

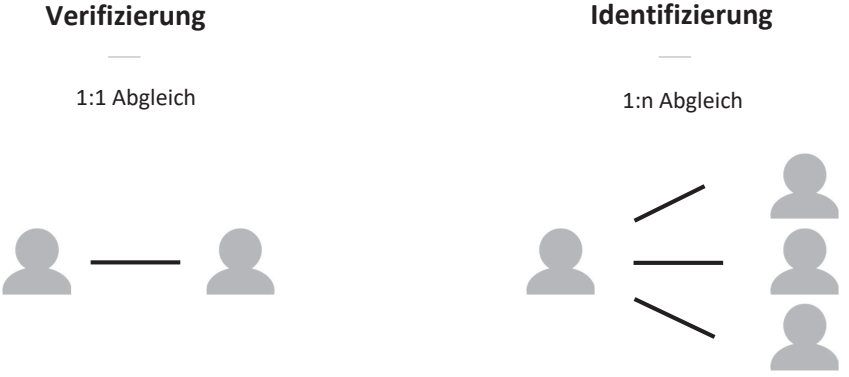

Abbildung 1: Verifizierung vs. Identifizierung

Die für die Strafverfolgung relevanten Szenarien betreffen vor allem solche der Identifikation. Zwar können Strafverfolgungsbehörden Gesichtserkennung auch im Modus der Verifikation einsetzen, etwa um bei einer polizeilichen Kontrolle die Identität des Betroffenen herauszufinden.[82] Diese Fälle sind jedoch deutlich unproblematischer, denn von der Verwendung automatisierter Gesichtserkennung zur Verifikation gehen sehr viel geringere Gefahren aus als bei der Identifikation. Insbesondere werden bei der

2017, 177, 181 f. Die Begriffe Identifikation und Verifikation sind in der technischen Literatur üblicher als Identifizierung und Verifizierung.

81 Vgl. etwa zum Angebot der Star Alliance *Rostalski/Weiss*, in: Hilgendorf/Roth-Isigkeit, Die neue Verordnung der EU zur Künstlichen Intelligenz, 2023, 35, 42.

82 Derzeit wird eine biometrisch basierte Überprüfung der Identität anhand der Fingerabdrücke vorgenommen. Im Rahmen des sog. Fast-ID-Verfahrens können digital aufgenommene Fingerabdrücke in Echtzeit im AFIS (automatisiertes Fingerabdruck-Identifizierungs-System) recherchiert werden.

Verifikation die Merkmale einer Person mit nur *einem einzigen* Datensatz abgeglichen, nicht auch mit den Datensätzen zahlreicher Unbeteiligter. Typischerweise hat Gesichtserkennung auch eine geringere Fehlerrate, wenn sie zur Verifikation verwendet wird, da die gescannte Person – etwa bei einer biometrischen Gesichtserkennung zur Passkontrolle – kooperiert und in einer gut beleuchteten Umgebung aus geringer Entfernung direkt in die Kamera schaut.[83] Dadurch hat die betroffene Person auch meist Kenntnis von der Maßnahme, während Identifikationen heimlich erfolgen können.

II. Entwicklung der automatisierten Gesichtserkennung

Computer waren dem Menschen schnell darin überlegen, Informationen zu speichern, abzurufen und komplexe mathematische Rechnungen ausführen. Das maschinelle Sehen (Computer vision), auf dem auch Gesichtserkennung basiert, war dagegen lange Zeit eine Aufgabe, an der Computer scheiterten.

1. Anfänge der Forschung

Am 19. August 1985 eröffnete Woodrow Wilson Bledsoe, der Präsident der Association for the Advancement of Artificial Intelligence (AAAI),[84] seine Ansprache an die Mitglieder mit einem Rückblick auf seinen ambitionierten Traum als junger Forscher. Sein Ziel war es gewesen, einen „mechanischen Computer-Freund" zu erschaffen:[85]

> *„Twenty-five years ago I had a dream, a daydream, if you will. A dream shared with many of you. I dreamed of a special kind of computer, which had eyes and ears and arms and legs, in addition to its ‚brain'. … [M]y dream was filled with the wild excitement of seeing a machine act like a human being, at least in many ways.*

83 *Li/Jain*, in: Li/Jain, Handbook of Face Recognition, 2011, 1, 3; *Tistarelli/Champod*, in: Tistarelli/Champod, Handbook of Biometrics for Forensic Science, 2017, 1, 5. Allerdings könnte auch bei der Passkontrolle (also in einer kontrollierten Umgebung) ohne Wissen der Betroffenen eine Identifizierung statt nur eine Verifikation durchgeführt werden.

84 Zum damaligen Zeitpunkt (und bis 2007) hieß die Vereinigung noch American Association for Artificial Intelligence.

85 *Bledsoe*, „I Had a Dream: AAAI Presidential Address", 19 August 1985, AI Magazine 1986, 57.

> *I wanted it to read printed characters on a page and handwritten script as well. I could see it, or a part of it, in a small camera that would fit on my glasses, with an attached earplug that would whisper into my ear the names of my friends and acquaintances as I met them on the street. … For you see, my computer friend had the ability to recognize faces…*"

Als Bledsoe in den 1960er-Jahren gemeinsam mit Helen Chan and Charles Bisson begann, eine computergestützte Gesichtserkennung zu entwickeln, war dieser Traum weit entfernt davon, Realität zu werden. Auf der Grundlage seiner bisherigen Arbeiten zur Mustererkennung begann der US-amerikanische Informatiker und Mathematiker zunächst mit dem Ziel, einem Computer beizubringen, zehn Gesichter zu erkennen.[86] Er wollte einem Computer eine Datenbank mit zehn Fotos von verschiedenen Menschen geben und sehen, ob er ihn dazu bringen könne, neue Fotos von jeder dieser Personen zu erkennen. Bald, so hoffte Bledsoe, würde man diese Zahl auf tausende Personen erhöhen zu können.[87] Was wie ein bescheidenes Bestreben klingt, war im Jahr 1963 ausgesprochen ehrgeizig und stellte sich als ein schwieriges Unterfangen heraus. Nach 13 Monaten Arbeit konnte der Computer kein einziges menschliches Gesicht erkennen.[88] Schwierigkeiten bereitete vor allem die Variabilität ein und desselben menschlichen Gesichts. Die Rotation des Kopfs, Lichtverhältnisse und Aufnahmewinkel können variieren, Menschen altern, Haare und Bart wachsen, und wer auf einem Foto ärgerlich schaut, kann auf dem nächsten breit grinsen.[89] Auch gab es keine einfache Standardmethode, um Fotografien zu digitalisieren, und daher auch keine digitalen Datenbanken, auf die Forschende hätten

86 *Bledsoe*, Proposal for a Study to Determine the Feasibility of a Simplified Face Recognition Machine, 1963, 2.

87 *Bledsoe*, Proposal for a Study to Determine the Feasibility of a Simplified Face Recognition Machine, 1963, 2 („Soon one would hope to extend the number of persons to thousands.").

88 *Bledsoe*, Facial Recognition Project Report, 1964, 2.

89 *Bledsoe*, Facial Recognition Project Report, 1964, 2; *Bledsoe*, The Model Method in Facial Recognition, Technical Report PRI 15, 1964, 1: „The variability is extensive. It includes: (1) Head rotation (from frontal, to profile), and tilt. (2) Lighting intensity and angle. (3) Photograph size (scale). (4) Facial expression. (5) Aging. (6) Hair growth".

zurückgreifen können.[90] Diese mussten zunächst Foto für Foto aufgebaut werden. Verwendet wurden ausschließlich Bilder von weißen Männern.[91]

Bledsoe kam zu der Überzeugung, dass es der vielversprechendste Weg zur automatisierten Gesichtserkennung war, ein Gesicht auf eine Reihe von Abständen und Beziehungen zwischen seinen wichtigsten Orientierungspunkten zu reduzieren: Augen, Ohren, Nase, Augenbrauen, Lippen. Dazu lokalisierten und notierten menschliche *Operators* die Koordinaten dieser Merkmale.[92] Aus diesen Koordinaten wurde eine Liste von 20 Entfernungen berechnet, etwa die Breite des Mundes, die Breite der Augen, der Abstand von Pupille zu Pupille. Zudem sollte eine größere Datenbank aufgebaut werden. Die *Operators* waren in der Lage, etwa 40 Bilder pro Stunde zu verarbeiten. Beim Aufbau der Datenbank wurde der Name der Person auf dem Foto mit der Liste der berechneten Abstände verknüpft und im Computer gespeichert. In der Erkennungsphase wurde das Set an Abständen mit den entsprechenden Abständen für jedes Foto verglichen. Der Computer lieferte dann eine Liste mit den am stärksten übereinstimmenden Datensätzen. Bledsoe bezeichnete dieses Vorgehen als „Mensch-Maschine-Technik" („man-machine technique"),[93] da eine menschliche Mitwirkung zwingend notwendig und eine vollautomatisierte Erkennung nicht möglich war. Der Algorithmus zur Erkennung der Gesichter war ein einfacher Abgleich der Abstände im Gesicht der zu identifizierenden Person mit den Abständen der Gesichter in der Datenbank. Der Computer war nicht für das Vermessen und Erkennen der Gesichter zuständig, sondern nur für die Verwaltung der Datenmengen; er war in diesem Sinne (noch) „blind".[94]

Einen großen Sprung in der Entwicklung computergestützter Gesichtserkennung machte der japanische Informatiker Takeo Kanade im Jahr 1973.[95] Mithilfe einer für damalige Verhältnisse enormen Datenbank von über 1000 digitalisierten Fotos entwickelte er das erste automatisierte Ge-

90 Die erste Digitalkamera wurde erst 1975 erfunden, siehe *Steven Sasson/Gareth Llyod*, „Electronic still camera" (U.S. Patent 4,131,919), U.S. Patent and Trademark Office, 1978. Zuvor mussten analoge Fotos manuell digitalisiert werden.

91 *Raviv*, Wired v. 21.1.2020, https://perma.cc/A7YR-RLDT.

92 Dieses Vorgehen beschreibt Bledsoe in *Bledsoe*, The Model Method in Facial Recognition, Technical Report PRI 15, 1964, 21.

93 *Bledsoe*, The Model Method in Facial Recognition, Technical Report PRI 15, 1964, 1.

94 *Meyer*, Regards Croisés 2020, 12, 16.

95 *Kanade*, Picture Processing System by Computer Complex and Recognition of Human Faces, 1973.

sichtserkennungssystem. Wie bei Bledsoe beruhte auch sein Ansatz darauf, prägnante Gesichtsmerkmale und deren Abstände zu erfassen (Feature-based approach). Ein Computerprogramm lokalisierte zunächst prägnante Gesichtsmerkmale wie Augenwinkel, Nasenlöcher und Kinnspitze und berechnete daraus verschiedene Gesichtsparameter, zum Beispiel den Abstand zwischen den Mundwinkeln oder zwischen Kinn und Nasenloch.[96] Diese Parameter verglich der Computer dann automatisiert und konnte so immerhin 15 von 20 Personen korrekt identifizieren.[97]

Erst Anfang der 1990er-Jahre gelang der nächste entscheidende Durchbruch mit dem ersten *voll*automatisierten Gesichtserkennungssystem. Dieses von Matthew Turk und Alex Pentland[98] entwickelte Verfahren, die *Eigenface*-Methode, war die Grundlage für eine Reihe von Weiterentwicklungen. Anders als frühere Ansätze, bei denen prägnante Gesichtsmerkmale und die Beziehung zwischen ihnen im Zentrum standen (Feature-based approaches), betrachtet ihre Methode das Gesicht als Ganzes. Mithilfe eines Trainingssets von Bildern wird zunächst ein Durchschnittsgesicht berechnet und dann der Unterschied jedes einzelnen Gesichts zu diesem Durchschnittsgesicht bestimmt. Darauf resultieren dann die „Eigenfaces": verschwommene, gesichtsähnliche Bilder mit Helligkeitsunterschieden (zum Durchschnittsgesicht), die über das ganze Gesicht verteilt sind. Allerdings ist diese Methode – wie auch schon die früheren Ansätze – sehr anfällig für Variationen in Lichtverhältnissen, Rotation und Skalierung des Gesichts, Gesichtsausdruck, Verdeckungen und Größe des Bildes. Die Erkennung funktioniert nur zuverlässig, wenn die Person bei jeder Bildaufnahme frontal in die Kamera blickt und die Beleuchtung ähnlich ist. Daher müssen die Bedingungen, unter denen die Bilder aufgenommen werden, sehr präzise kontrolliert werden. Die Erkennung eines Gegenübers auf der Straße, wie bereits Bledsoe sich dies vorstellte, ist damit nicht möglich.

96 *Kanade*, Picture Processing System by Computer Complex and Recognition of Human Faces, 1973, 77 ff., 85 ff.

97 *Kanade*, Picture Processing System by Computer Complex and Recognition of Human Faces, 1973, 91.

98 *Turk/Pentland*, Proceedings of the IEEE Computer Science Conference on Computer Vision and Pattern Recognition 1991, 586; *Turk/Pentland*, Journal of Cognitive Neuroscience 1991, 71. Ihr Ansatz baute auf der Arbeit von Lawrence Sirovich und Michael Kirby auf, *Sirovich/Kirby*, Journal of the Optical Society of America 1987, 519.

2. Nutzbarmachung für die Strafverfolgung

Um die Forschung zu Gesichtserkennung aus dem Computerlabor zu holen und auch in der Praxis der Strafverfolgung, Nachrichtendienste und Sicherheitsbehörden nutzbar zu machen, rief das US-Verteidigungsministerium 1993 das FERET-Programm ins Leben.[99] Das Programm stellte eine für damalige Verhältnisse umfangreiche Datenbank mit etwa 2.400 Bildern zur Verfügung und unterstützte weitere Forschung. Diese Datenbank ermöglichte es auch, die Leistungsfähigkeit verschiedener Gesichtserkennungsalgorithmen zu testen und zu vergleichen. Da die Entwicklungsteams verschiedene Datenbanken verwendeten, war ein Vergleich zuvor schwierig gewesen. Mit dem FERET-Programm begann auch die Kommerzialisierung automatisierter Gesichtserkennung, die, wie beabsichtigt, zahlreiche Innovationen und Kostensenkungen mit sich brachte. In den darauffolgenden Jahren spornten weitere Tests und Wettbewerbe die Entwicklung an, vor allem die Face Recognition Vendor Tests des US-amerikanischen National Institute of Standards and Technology (NIST), die noch heute stattfinden.[100]

Der erste bekannte Großeinsatz von Gesichtserkennung erfolgte beim Super Bowl im Frühjahr 2001 in Tampa, Florida.[101] Kameras scannten die über 70.000 Football-Fans im Stadion und glichen sie mit polizeilichen Fahndungslisten ab. Ob von den 19 Treffern tatsächlich einer korrekt war, blieb offen; zu einer Verhaftung kam es jedenfalls nicht.[102] Gleichwohl rüstete Tampa daraufhin im Sommer 2001 die Videokameras in der Innenstadt zur „Smart CCTV" (intelligenten Videoüberwachung) mit Gesichtserkennung auf. Da sich Fehlalarme häuften und die erhofften Treffer ausblieben, schaltete die Polizei das Programm ab.[103]

Dennoch verbreiteten sich Gesichtserkennungssysteme mit rasanter Geschwindigkeit in Folge der Terroranschläge vom 11. September 2001.[104] Bereits zwei Wochen nach den Attentaten warb ein Unternehmen damit, die

99 National Institute of Standards and Technology, https://perma.cc/3EWX-WC9B. Einige Behörden wie das FBI hatten wohl auch zuvor schon Forschung zu Gesichtserkennung gefördert, ohne dass dies öffentlich bekannt gemacht wurde.

100 Zu den Ergebnissen der Tests des NIST auch Kapitel I. E. IV. 4.

101 *McCullagh*, Wired v. 2.1.2001, https://perma.cc/9ES3-7Q8W.

102 *Slevin*, The Washington Post v. 1.2.2001, https://perma.cc/CMH5-YGJV.

103 *Gates*, Culture Unbound Journal of Current Cultural Research 2010, 67, 85.

104 *Gates*, Cultural Studies 2006, 417, 425; *Tomaszewska-Michalak*, Studia Politologiczne 2022, 123, 125.

Bevölkerung mit Gesichtserkennung vor den „Faces of Terror" zu schützen.[105] Mit Gesichtserkennungstechnologie, so das Versprechen, hätte man die Terroristen bereits beim Check-in identifizieren und dadurch die Anschläge verhindern können. Tatsächlich wurden in den folgenden Monaten vor allem die Flughäfen biometrisch aufgerüstet und mit Fingerabdruck-Scannern und Kameras für Gesichtserkennung ausgestattet.[106] Auch in der Strafverfolgung breitete sich die Technologie aus.[107] Doch selbst die Hersteller von Gesichtserkennungssystemen räumten ein: Eine Erkennung sei nur zuverlässig möglich, wenn die gesuchte Person frontal in die Kamera blickt und wenn sie überhaupt mit Foto als Verdächtiger in einer Datenbank erfasst ist.[108]

Einem dieser Hindernisse sollte bereits kurz darauf abgeholfen werden. Die nach 9/11 gestiegene Bereitschaft der Bevölkerung, ihre Privatheit gegen mehr Sicherheit einzutauschen, bereitete in den nächsten Monaten und Jahren den Boden für zahlreiche Gesetze, die es ermöglichten, in großem Umfang Daten (darunter Bilder) zu erheben, zu sammeln, zu vernetzen und zu verwerten.[109] So sah etwa das Programm „US-VISIT" (United States Visitor and Immigrant Status Indicator Technology) vor, dass alle Nicht-US-Bürger bei der Einreise digital fotografiert und ihre Fingerabdrücke erfasst werden mussten.

3. Durchbruch durch große Datenbestände und maschinelles Lernen

Der technische Fortschritt ließ etwas länger auf sich warten. Doch in den 2010er-Jahren traf Gesichtserkennung dann unerwartet auf eine andere technologische Innovation: Social Media. Viele Nutzerinnen und Nutzer waren nicht nur bereit dazu, sondern begierig darauf, etliche Fotos von sich auf Facebook und Instagram zu veröffentlichen, in allen Facetten, aus allen Blickwinkeln, zu verschiedenen Tageszeiten, mit Sonnenbrille, mit und ohne Bart, mit und ohne Make-up – ein Traum für jeden Entwickler von Gesichtserkennungsalgorithmen. 2014 verkündete Facebook, einen Algo-

105 *Gates*, Cultural Studies 2006, 417, 425.
106 Siehe nur *ACLU*, Pressemitteilung vom 20.11.2001, https://perma.cc/R8XV-QAKR.
107 *Watkins*, The New York Times v. 8.9.2021, https://perma.cc/LB56-EABB.
108 Siehe hierzu *O'Connor*, Bender's Immigration Bulletin 2002, 150, 154.
109 Beispielhaft genannt sei nur der USA Patriot Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001), der die Überwachungsbefugnisse im Inland stark ausweitete.

rithmus entwickelt zu haben, dessen Erkennungsrate auch in nicht-kontrollierten Settings an die menschliche Erkennungsfähigkeit heranreiche, sie teilweise sogar übertreffe.[110] Die Software *DeepFace* war mit über 4 Millionen Fotos von rund 4.000 Personen trainiert und anschließend anhand der bekannten Datenbank *Labeled Faces in the Wild* (LFW) evaluiert worden. Bei diesem Test erreichte *DeepFace* eine Erkennungsrate von 97,35 %, Menschen erkannten rund 97,5 % der Gesichter korrekt. Zwar müssen diese Ergebnisse kritisch eingeordnet werden: Die LFW-Datenbank enthält lediglich 13.000 Fotos, die zudem nicht sehr divers sind (wenige Frauen, kaum Kinder, kaum Menschen über 80 Jahren, viele Ethnien kaum oder nicht vertreten).[111] Auch wurde die Leistungsfähigkeit von *DeepFace* lediglich mit Blick auf 1:1-Abgleiche getestet. Mit zunehmender Anzahl von Bildern und beim Einsatz zur Identifizierung (1:n Abgleich) sinkt die Erkennungsleistung von Gesichtserkennungsalgorithmen beträchtlich.[112] Dennoch war diese drastische Verbesserung ein Meilenstein.

Entscheidend für diesen Fortschritt war neben der schieren Anzahl von Trainingsdaten (Bildern) das Werkzeug, um diese überhaupt erst sinnvoll verarbeiten zu können: maschinelles Lernen. Das maschinelle Lernen ist gegenwärtig eines der wichtigsten Teilgebiete der Künstlichen Intelligenz und ein Oberbegriff für die künstliche Generierung von Wissen aus Erfahrung.[113] Anstatt dem System vorzugeben, was es tun soll, lernt es selbst

110 *Taigman/Yang/Ranzato/Wolf*, Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition 2014, 1701.

111 Siehe den Disclaimer auf der Webseite von Labeled Faces in the Wild, https://perma.cc/4PBK-MX5W („Many groups are not well represented in LFW. For example, there are very few children, no babies, very few people over the age of 80, and a relatively small proportion of women. In addition, many ethnicities have very minor representation or none at all.").

112 Bei Tests anhand von größeren Datensätzen zeigte sich wiederholt, dass die bei Tests in der LFW-Datenbank erzielten „beinahe-perfekten" Erkennungsraten von Gesichtserkennungsalgorithmen nicht replizierbar waren, siehe nur *Kemelmacher-Shlizerman/Seitz/Miller/Brossard*, Proceedings of the IEEE Conference of Computer Vision and Pattern Recognition 2016, 4873, 4847 („Algorithms that achieve above 95% performance on LFW (equivalent of 10 distractors in our plots), achieve 35-75% identification rates with 1M distractors."). Siehe auch *Zulqarnain Gilani/Mian*, Proceedings of the IEEE Conference of Computer Vision and Pattern Recognition 2018, 1896, 1896 f., 1898.

113 *Norvig/Russell*, Artificial Intelligence: A Modern Approach, Global Edition, 4. Aufl., 2021, 670 ff. (insbesondere: „An agent is learning if it improves its performance after making observations about the world. […] When the agent is a computer, we call it machine learning: a computer observes some data, builds a model based on the

durch Versuch und Irrtum.[114] Auf Gesichtserkennung übertragen bedeutet das: Das System lernt selbst, auf welche Gesichtsmerkmale es achten muss, um Personen zu erkennen.

Auch andere Technologiegiganten wie IBM, Microsoft und Amazon setzten auf enorme Datenmengen und maschinelles Lernen, um Gesichtserkennungsalgorithmen zu trainieren. Im Zuge der Black-Lives-Matter-Proteste und ihrer Kritik an rassistischer Polizeigewalt entfachte die Kritik an Gesichtserkennung jedoch neu und die großen Technologiekonzerne verkündeten im Jahr 2020 kurz nacheinander, dass sie ihre Systeme nicht an Polizeibehörden verkaufen würden.[115] Zumindest solange der Einsatz von Gesichtserkennung nicht durch ein nationales Gesetz geregelt sei, wolle man die Technologie nicht in die Hände der Strafverfolgungsbehörden geben.[116] Ein US-weites Gesetz zur Verwendung von Gesichtserkennung durch die Polizei wurde jedoch bis heute nicht erlassen.[117]

4. Neue Akteure

Statt der Tech-Giganten trat ein neuer Akteur ins Bild, der revolutionäre Maßstäbe setzte: das Start-Up *Clearview AI*. Der Durchbruch war allerdings weniger ein technologischer als vielmehr ein ethischer.[118] Das Unternehmen war in die Schlagzeilen geraten, nachdem bekannt geworden war, dass es von öffentlichen Webseiten wie Facebook, Instagram, Twitter

---

Machine learning data, and uses the model as both a hypothesis about the world and a piece of software that can solve problems.").

114 Treffend auch *Tufekci* in Coded Bias Discussion Guide 2021, 9, https://perma.cc/79PM-RZ2B: „There are two ways in which you can program computers. One of them is more like a recipe. You tell the computer to do this, do this, do this, do this. That's been the way we've programmed computers almost from the beginning. Now there's another way. That way is feeding the computer lots of data and then the computer learns to classify by digesting this data."

115 *Denham*, The Washington Post v. 11.6.2020, https://perma.cc/2ENX-EA99. Jedenfalls IBM hat sich zwischenzeitlich jedoch umentschieden und bietet Strafverfolgungsbehörden nun doch Gesichtserkennungssoftware an, *Wilding*, The Verge v. 31.8.2023, https://perma.cc/Q533-Z8AV.

116 *Greene*, The Washington Post v. 11.6.2020, https://perma.cc/Q255-8FPL.

117 Zur unübersichtlichen und uneinheitlichen Rechtslage *Rabinowicz*, Harvard Journal of Law and Technology JOLT Digest, 4.5.2023, https://perma.cc/CU57-RQ9S.

118 So die zutreffende Einschätzung der New York Times Reporterin *Kashmir Hill* in *Mineo*, The Harvard Gazette v. 26.10.2023, https://perma.cc/38QG-HF26 („Clearview made an ethical breakthrough, not a technological one.").

und YouTube Milliarden von Fotos mit Gesichtern zusammengetragen und in einer per Gesichtserkennung durchsuchbaren Datenbank gespeichert hatte.[119] Über 30 Milliarden Bilder hat *Clearview AI* so mittlerweile gesammelt.[120] In einer App kann ein beliebiges Foto hochgeladen und so der Name der abgebildeten Person ermittelt werden. Hunderte Polizeibehörden in den USA setzen auf die App, Anfang 2023 war sie bereits für 1 Million Suchläufe verwendet worden.[121] Unterdessen entwickelt *Clearview AI* weitere Anwendungen für seine Gesichtserkennungstechnologie. Es wird zukünftig seine Gesichtserkennungstechnologie in Augmented-Reality-Brillen integrieren, verbunden mit der *Clearview AI*-App und der Datenbank mit 30 Milliarden Gesichtern.[122] Mit dieser Brille soll es für Polizisten möglich sein, durch die Straßen zu gehen und gesuchte Personen zu identifizieren.[123]

Bledsoe schloss seine Ansprache vom 19. August 1985 an die Mitglieder der Association for the Advancement of Artificial Intelligence mit den Worten: „I have told you about my dream, have offered advice for young researchers, and have offered my opinion on important areas of AI research. But of all the predictions that I could make, the one that I'm most sure about is that we will again be *surprised*."[124] Und überrascht wäre er. Sein jahrelanger Traum von einem „mechanischen Computer-Freund", der Menschen auf der Straße erkennt, ist Realität geworden.

III. Ablauf einer Erkennung

Im Gegensatz zu Menschen vergleicht die automatisierte Gesichtserkennung nicht die Gesichter selbst, sondern numerische Darstellungen der Gesichter, sogenannte Face Embeddings[125]. Face Embeddings sind Vekto-

119 *Hill*, The New York Times v. 18.1.2020, https://perma.cc/C4H9-NC6H.

120 Vgl. die Webseite von *Clearview AI*, How We Store and Search 30 Billion Faces, https://perma.cc/26PG-KURE.

121 *Clayton/Derico*, BBC v. 27.3.2023, https://perma.cc/Q97Q-YFPQ.

122 *Hill*, Your Face Belongs to Us, 249 f. Über China wird berichtet, dass die Polizei an einigen Orten bereits 2018 Sonnenbrillen mit integrierter Gesichtserkennung nutzte, *Mozur*, The New York Times v. 8.7.2018, https://perma.cc/BC7A-GUN5.

123 *Hill*, Your Face Belongs to Us, 249 f.

124 *Bledsoe*, „I Had a Dream: AAAI Presidential Address", 19 August 1985, AI Magazine 1986, 57, 61.

125 Der Begriff Template wird ebenfalls gebraucht, neuere Publikationen verwenden hingegen überwiegend den Begriff Embeddings.

ren, die Gesichtsmerkmale repräsentieren.[126] Zur Extraktion der Embeddings werden heutzutage tiefe, künstliche neuronale Netze verwendet, die vorab mit Millionen oder auch teilweise Milliarden von Bildern trainiert wurden;[127] eine anschauliche Erklärung wie sie genau zustande kommen, ist aufgrund der Komplexität (teilweise Milliarden Rechenoperationen pro Embedding-Generierung) nicht möglich. Diese Embeddings werden dann miteinander abgeglichen, etwa das Embedding des Gesichts eines Tatverdächtigen mit den Embeddings der Gesichter in einer Datenbank. Je geringer die Entfernung zwischen den Vektoren, desto mehr ähneln sich die Embeddings.[128] Liegt die Ähnlichkeit oberhalb des eingestellten Schwellenwerts, dann werden die beiden Embeddings und damit die ihnen zugrunde liegenden Gesichter als übereinstimmend eingestuft.[129]

Wie hoch oder niedrig der Schwellenwert eingestellt werden sollte, unterscheidet sich je nach Einsatzszenario.[130] Je geringer er angesetzt wird, desto mehr falsche Treffer liefert das System.[131] Bei einem Wert von 75 % würden beispielsweise alle Personen angezeigt, die der gesuchten Person so weit ähneln (genauer gesagt: deren Embedding dem der gesuchten Person so weit ähnelt). Dadurch steigt die Gefahr einer Fehlidentifizierung. Ein solcher geringer Schwellenwert hat aber den Vorteil, dass der Gesuchte auch anhand von Bildern erkannt werden könnte, die eine suboptimale Qualität haben oder unter schlechten Lichtverhältnissen entstanden sind.

126 Vgl. nur *Schroff/Kalenichenko/Philbin*, Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition 2015, 815, 821.

127 Siehe etwa bei *Knoche/Hörman/Rigoll*, Leibniz Transactions on Embedded Systems 2022, arXiv, 1, 6. Allgemein zum Training von Bilderkennungssystemen Leupold/Wiebe/Glossner/*Baum*, IT-Recht, 4. Aufl. 2021, Teil 9.1 Technische Grundlagen, Rn. 29 ff. Siehe auch *Tan/Guo*, in: Li/Jain/Deng, Handbook of Face Recognition, 2024, 3, 6 ff.

128 Siehe beispielhaft bei *Schroff/Kalenichenko/Philbin*, Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition 2015, 815 („The network is trained such that the squared L2 distances in the embedding space directly correspond to face similarity: faces of the same person have small distances and faces of distinct people have large distances.").

129 Vgl. *Li/Jain*, in: Li/Jain, Handbook of Face Recognition, 2011, 1, 3.

130 Beispielsweise kann es beim Sortieren von Fotos auf dem eigenen Smartphone sinnvoll sein, wenn ein geringer Schwellenwert gilt, denn dann findet die Gesichtserkennung womöglich auch Bilder, auf denen die gewünschte Person schräg von der Seite oder bei Dunkelheit aufgenommen wurde; gleichzeitig können in einem solchen Anwendungsszenario die falschen Treffer ohne Probleme manuell aussortiert werden.

131 Ausführlich zu den Fehlerraten von Gesichtserkennung sogleich unter III.

Je höher der Schwellenwert hingegen angesetzt wird, desto weniger wahrscheinlich ist es, dass falsche Matches generiert werden.[132] Dadurch sinkt die Gefahr von Fehlidentifizierungen durch die Polizei, da das System von vornherein weniger (mögliche) Treffer vorschlägt.

IV. Fehlerraten

„Data is destiny."
– Joy Buolamwini[133]

Automatisierte Gesichtserkennung ist nicht fehlerfrei. Wie auch bei anderen Anwendungen der Künstlichen Intelligenz und des maschinellen Lernens beeinflussen Anzahl, Qualität und Diversität der Trainingsdaten entscheidend die Leistungsfähigkeit des Gesichtserkennungssystems. Auch die Qualität der Input-Daten, also die zum Abgleich herangezogenen Lichtbilder, wirkt sich auf die Leistung aus. Dieser Abschnitt erläutert zunächst die Arten von Fehlern (1.) und ihre Ursachen (2.). Zudem wird darauf eingegangen, unter welchen Umständen eine höhere Fehlerrate auch erwünscht sein kann (3.). Darauf folgt ein Überblick zum aktuellen Stand der Leistungsfähigkeit der Technologie (4.). Zuletzt wird näher betrachtet, ob und aus welchem Grund sich die Fehlerraten für unterschiedliche Bevölkerungsgruppen unterscheiden (5.).

1. Arten von Fehlern

Bei dem Einsatz von Technologien zur automatisierten Gesichtserkennung können zwei Arten von Fehlern entstehen: falsche Treffer (False positives) und falsche Nichttreffer (False negatives). Wenn die Technologie eine Person fälschlicherweise nicht identifiziert, handelt es sich um einen falschen Nichttreffer, bei einer Fehlidentifizierung um einen falsch-positiven Treffer.

132 Vgl. auch *Grother/Ngan/Hanaoka*, Face Recognition Technology Evaluation (FRTE) Part 2: Identification, NISTIR 8271 Draft Supplement, 2023, 10 f., 31.
133 Coded Bias Discussion Guide 2021, 9, https://perma.cc/79PM-RZ2B.

		Tatsächlich	
		Person A	Nicht Person A
Vorhersage des Systems	Person A	*True Positive*	*False Positive*
	Nicht Person A	*False Negative*	*True Negative*

Abbildung 2: True positives, False positives, True negatives, False negatives

Wenn also Person A auf dem vorhandenen Bildmaterial zu sehen ist, die Technologie sie aber nicht als Person A erkennt, ist dies ein falscher Nichttreffer (False negative). Zeigt das Bildmaterial hingegen Person B, die Technologie wirft aber das Ergebnis aus, dass die Bilder Person A zeigen, dann liegt ein falsch-positiver Treffer (False positive) vor.

a) Falsche Nichttreffer (False negatives)

Ein falscher Nichttreffer bedeutet in allen Einsatzszenarien automatisierter Gesichtserkennung „nur", dass die Technologie das gewünschte Ergebnis nicht liefert.[134] Gesichtserkennung ist in diesem Fall dann lediglich kein hilfreiches Ermittlungstool, es entstehen aber grundsätzlich keine Risiken für den Verdächtigen oder Unbeteiligte.

b) Falsche Treffer (False positives)

Ein falsch-positiver Treffer bei der Identitätsermittlung bedeutet hingegen, dass ein Unbeteiligter fälschlicherweise als der Verdächtige identifiziert

134 Beim Einsatz von Gesichtserkennung zur Ermittlung der Identität eines unbekannten Verdächtigen etwa wird dann diese Person, obwohl sie in der Datenbank vorhanden ist, nicht als Treffer angezeigt. Beim Einsatz von Gesichtserkennung zur Echtzeit-Fahndung wird der Gesuchte nicht erkannt (und daher kein Alarm bei der Polizei ausgelöst), obwohl er tatsächlich an der mit Gesichtserkennung ausgestatteten Kamera vorbeigelaufen ist.

wird.[135] Das kann dazu führen, dass er Adressat strafprozessualer Ermittlungsmaßnahmen wird. Wie bereits erwähnt, gibt es bereits eine Reihe solcher Fälle in den USA, in denen es zu Festnahmen Unschuldiger kam, die fälschlicherweise von einer Gesichtserkennungssoftware als Verdächtige einer Straftat identifiziert wurden.[136]

c) Messung

Wie fehlerbehaftet ein System ist, kann mit der Falschakzeptanzrate (False acceptance rate) und der Falschrückweisungsrate (False rejection rate) angegeben werden. Die False acceptance rate ist die Rate (Prozentsatz), mit der die aus den Gesichtern zweier verschiedener Personen extrahierten Merkmalssätze als übereinstimmend gewertet werden; vereinfacht also die Rate, mit der fälschlicherweise zwei unterschiedliche Personen als Match (False positive) gewertet werden.[137] Die False rejection rate ist der Prozentsatz der Fälle, in denen eine Person nicht mit ihren eigenen vorhandenen Referenzvorlagen als übereinstimmend gewertet wird; mit anderen Worten:

135 Falsch-positive Treffer wirken sich in den Einsatzszenarien jeweils auf verschiedene Weise aus. Im Falle einer Observation mittels Gesichtserkennungstechnologie bedeutet eine falsch-positive Erkennung, dass Videomaterial fälschlicherweise einem Verdächtigen zugeordnet wird. Bleibt der Fehler unerkannt, ziehen die Strafverfolgungsbehörden womöglich falsche Schlüsse aus einem Verhalten oder Bewegungsmuster, das in Wirklichkeit gar nicht von dem Verdächtigen stammt. Bei der Echtzeit-Fahndung kann ein falsch-positives Match bedeuten, dass ein Unbeteiligter angehalten und festgenommen wird.

136 Zu diesen Fällen auch ausführlich Kapitel III. B. I. 1. Zu der Frage, ob in diesen Fällen der Fehler nicht eher bei den Polizisten als bei der Technologie lag Kapitel III. B. II. Beim Einsatz von Echtzeit-Gesichtserkennung zur Lokalisierung eines Verdächtigen bedeutet ein falsch-positiver Treffer hingegen, dass ein unbeteiligter Passant fälschlicherweise als übereinstimmend mit dem Gesuchten gewertet wird; er wird dann möglichweise von der Polizei angehalten, aufgefordert sich auszuweisen oder festgenommen.

137 *Wei/Li*, in: Tistarelli/Champod, Handbook of Biometrics for Forensic Science, 2017, 177, 182. In der Fachliteratur ist die Terminologie uneinheitlich, siehe etwa *Wei/Li*, in: Tistarelli/Champod, Handbook of Biometrics for Forensic Science, 2017, 177, 182 (False acceptance rate und False rejection rate); *Brauckmann/Busch*, in: Li/Jain, Handbook of Face Recognition, 2011, 639, 642 (False nonmatch rate und False match rate). Die Rate bezieht sich immer auf die Anzahl der falschen Matches bei einem bestimmten Schwellenwert.

der Prozentsatz der echten Matches, die aber nicht als solche erkannt werden (False negatives).[138]

2. Ursachen von Fehlern

a) Unterschiedliche Leistungsfähigkeit verschiedener Systeme

Die Leistungsfähigkeit eines Gesichtserkennungssystems hängt von verschiedenen Faktoren ab. Zunächst unterscheiden sich die Algorithmen verschiedener Entwickler (und teilweise sogar ein und desselben Entwicklers) in ihrer Performance;[139] insbesondere die Qualität und Diversität der Trainingsdaten haben einen großen Einfluss auf die Fehlerrate. Je mehr Trainingsdaten verwendet werden und je unterschiedlicher diese sind (etwa mit Blick auf Geschlecht, Ethnie und Alter), desto robuster und weniger fehleranfällig sind die Systeme.[140]

b) Unkooperatives Setting

Auch haben Beleuchtung, Aufnahmewinkel, Gesichtshaltung, Gesichtsausdruck und Bewegung einen großen Effekt auf die Erkennungsleistung.[141] Insgesamt sind daher die Fehlerraten in kooperativen Benutzerszenarien (kontrollierte Aufnahmebedingungen und Mitwirkung des Betroffenen) deutlich geringer als in nicht-kooperativen Benutzerszenarien.[142] Ein Gesichtserkennungssystem wird also wahrscheinlicher einen Fehler machen, wenn es einen Täter identifizieren soll, der bei Dämmerung von schräg oben von einer Überwachungskamera gefilmt wurde als bei einer automati-

138 *Wei/Li*, in: Tistarelli/Champod, Handbook of Biometrics for Forensic Science, 2017, 177, 182.

139 *Grother/Ngan/Hanaoka*, Face Recognition Technology Evaluation (FRTE) Part 2: Identification, NISTIR 8271 Draft Supplement, 2023, 9. Siehe auch bereits *Grother/Quinn/Ngan*, Face In Video Evaluation (FIVE), 2017, 14, die in der Auswahl des Algorithmus' den wichtigsten Einflussfaktor für die Erkennungsgenauigkeit sehen.

140 Zu höheren Fehlerraten für einige Bevölkerungsgruppen (und damit insgesamt höherer Fehleranfälligkeit) bei vielen Gesichtserkennungssystemen siehe Kapitel I. E. IV. 5.

141 *Li/Jain*, in: Li/Jain, Handbook of Face Recognition, 2011, 1, 3.

142 Zu dieser Unterscheidung auch *Li/Jain*, in: Li/Jain, Handbook of Face Recognition, 2011, 1, 3 (*cooperative* vs. *non-cooperative*).

sierten Passkontrolle am Flughafen, bei der die Person in gut beleuchtetem Umfeld direkt in die Kamera blickt. In den für die Strafverfolgung relevanten Einsatzszenarien stammen die Aufnahmen, auf denen der Verdächtige erkannt werden soll, meist aus einem nicht-kooperativen Setting. Bei der Identitätsermittlung werden Fotos von Überwachungskameras oder Smartphones von Zeugen, auf denen die Straftat festgehalten wurde, herangezogen.

c) Qualität der abzugleichenden Bilder

Zudem hängt die Leistung stark von der Bildqualität der Aufzeichnungen ab, die abgeglichen werden. Eine schlechte Qualität macht die Erkennung deutlich schwieriger.[143] Bei der Verwendung von Gesichtserkennung zur Identitätsermittlung haben die in der Datenbank zum Abgleich gespeicherten Lichtbilder weit überwiegend eine sehr hohe Qualität, da sie unter kontrollierten Bedingungen (erkennungsdienstliche Maßnahmen) aufgenommen wurden.[144] Die von Smartphones oder Überwachungskameras erstellten Aufzeichnungen des Tatverdächtigen wiederum können dagegen von schlechterer Qualität sein.

d) Alterung und Gesichtsabnutzung

Ein großer Zeitabstand zwischen den zu vergleichenden Bildern erhöht die Wahrscheinlichkeit, dass das Gesichtserkennungssystem einen Verdächtigen nicht erkennt, obwohl er in der Datenbank gespeichert ist (False negative).[145] Das liegt daran, dass sich das Gesicht mit dem Alter verändert;

143 Siehe nur *Grother/Ngan/Hanaoka*, Face Recognition Technology Evaluation (FRTE) Part 2: Identification, NISTIR 8271 Draft Supplement, 2023, 9; *Wei/Li*, in: Tistarelli/Champod, Handbook of Biometrics for Forensic Science, 2017, 177, 182.

144 Bei den in der polizeilichen Datenbank INPOL gespeicherten Lichtbildern beispielsweise handelt es sich zum größten Teil um Porträtfotos, die im Rahmen einer erkennungsdienstlichen Maßnahme erstellt wurden. Nur vereinzelt werden auch „uncontrolled images" aus Überwachungsvideos gespeichert, wenn kein anderes Bild der Person verfügbar ist, Summary report of the project „Towards the European Level Exchange of Facial Images" (TELEFI) 2021, 75, https://perma.cc/T6NE-GTRV.

145 *Grother/Ngan/Hanaoka*, Face Recognition Technology Evaluation (FRTE) Part 2: Identification, NISTIR 8271 Draft Supplement, 2023, 10 f.

typischerweise geschieht dies graduell, Umstände wie etwa verstärkter Drogenkonsum können dies jedoch enorm beschleunigen und dadurch die Erkennung stark erschweren.[146] Auch bei Kindern und Jugendlichen kann sich das Gesicht und damit die Merkmalsausprägung in kürzerer Zeit stark verändern, sodass bei ihnen vermehrt zu erwarten ist, dass sie fälschlicherweise nicht erkannt werden.[147]

e) Größe der Datenbank

Je mehr Personen sich in einer Datenbank befinden, desto wahrscheinlicher ist es, dass falsche Matches generiert werden.[148] Denn mit einer steigenden Anzahl an Personen steigt auch die Wahrscheinlichkeit, dass sich mehr und mehr Personen mit einer ähnlichen Gesichtsmerkmalsausprägung in der Datenbank befinden, die das System nicht auseinanderhalten kann.

f) Gewählter Schwellenwert

Die Fehlerrate hängt aber auch von dem eingestellten Schwellenwert ab. Wird lediglich ein geringer Schwellenwert eingestellt und damit nur eine geringere Übereinstimmung der den Bildern zugrunde liegenden Embeddings gefordert, generiert das Gesichtserkennungssystem mehr falsche Matches. Dadurch ergibt sich eine höhere False acceptance rate als bei einem höheren Schwellenwert. Wird andererseits jedoch ein höherer Schwellenwert eingestellt, ist es wahrscheinlicher, dass (fälschlicherweise)

146 *Yadav/Kohli/Pandey/Singh/Vatsa/Noore*, Proceedings of the IEEE Winter Conference on Applications of Computer Vision 2016, 1; *Grother/Ngan/Hanaoka*, Face Recognition Technology Evaluation (FRTE) Part 2: Identification, NISTIR 8271 Draft Supplement, 2023, 11.

147 *Grother/Ngan/Hanaoka*, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, 2019, 17.

148 *Grother/Ngan/Hanaoka*, Face Recognition Technology Evaluation (FRTE) Part 2: Identification, NISTIR 8271 Draft Supplement, 2023, 10, 34. *Brauckmann/Busch*, in: Li/Jain, Handbook of Face Recognition, 2011, 639, 644; *Phillips/Grother/Micheals*, in: Li/Jain, Handbook Handbook of Face Recognition, 2011, 551, 569.

kein Match generiert wird, obwohl sich die gesuchte Person in der Datenbank befindet.[149]

3. „Erwünschte" Fehler

Ein geringerer Schwellenwert und damit eine höhere False acceptance rate kann in bestimmten Situationen aber sogar sinnvoll sein. Bei der alltäglichen Verwendung von Gesichtserkennung, um Fotos auf dem Smartphone zu sortieren (z. B. alle Bilder von Person A) kann es nützlich sein, eine höhere False acceptance rate einzustellen, um auch Bilder zu finden, bei denen die Person bei schlechter Beleuchtung oder aus einem ungünstigen Winkel fotografiert wurde. Die anderen Personen, die aufgrund der niedrigeren Ähnlichkeitsrate dann ebenfalls zugeordnet werden, können manuell aussortiert werden.

Im Rahmen der Strafverfolgung kann dies unter Umständen ebenfalls sinnvoll sein. Zumindest bei besonders gewalttätigen und gefährlichen Verdächtigen, bei denen die Polizei keinerlei Hinweis auf die Identität hat, könnte es wünschenswert sein, für die automatisierte Gesichtserkennung Bilder zu verwenden, die sehr unscharf sind oder aus einem ungünstigen Winkel aufgenommen wurden, auch wenn die Ähnlichkeitsschwelle womöglich sehr niedrig angesetzt werden müsste, um überhaupt Übereinstimmungen mit einem solchen Bild zu erzielen. Auf diese Weise könnte die Polizei zumindest einen ersten Ermittlungsansatz haben, auch wenn das bedeutet, dass sie Dutzende von unschuldigen Personen manuell oder nach zusätzlichen Ermittlungen aussortieren muss.[150]

---

149 Zu diesem Trade-off zwischen falschen Treffern (False positives) und falschen Nichttreffern (False negatives) sogleich im nächsten Abschnitt.

150 Vgl. *Grother/Ngan/Hanaoka*, Face Recognition Technology Evaluation (FRTE) Part 2: Identification, NISTIR 8271 Draft Supplement, 2023, 10. Dies gilt insbesondere für Situationen, in denen es entscheidend ist, den Verdächtigen schnell zu finden. So lag der Fall etwa bei den Terroranschlägen auf den Boston-Marathon im April 2013; siehe zum Folgenden *Klontz/Jain*, A case study on unconstrained facial recognition using the Boston marathon bombings suspects, Technical Report MSU-CSE-13-4, 2013, 1. Nach dem Anschlag waren die Strafverfolgungsbehörden nicht in der Lage, die beiden Verdächtigen durch Gesichtserkennung zu identifizieren, obwohl beide Täter in der Datenbank gespeichert haben. Das Federal Bureau of Investigation (FBI) veröffentlichte Fotos und Videos der beiden Verdächtigen und rief die Bevölkerung zur Mithilfe bei der Identifizierung auf. Dadurch wussten die Täter, dass sie unter Verdacht standen und starteten einen Fluchtversuch, der zu

Es besteht ein Trade-off zwischen falschen Treffern (False positives) und falschen Nichttreffern (False negatives).[151] Je niedriger der Schwellenwert angesetzt wird, desto mehr falsch-positive Treffer werden generiert. Ein höherer Schwellenwert verringert zwar solche falsch-positiven Treffer, dies hat jedoch den Preis, dass fälschlicherweise auch echte Treffer nicht als solche erkannt werden.

4. Stand der Technik

Der folgende Überblick zeigt den aktuellen Stand der Technik mit Blick auf die Leistungsfähigkeit (Fehlerraten) von Gesichtserkennungssystemen. Die Technologie hinter der automatisierten Gesichtserkennung entwickelt sich jedoch kontinuierlich und mit rasanter Geschwindigkeit weiter. Ein solcher Überblick ist daher zwangsläufig nur eine Momentaufnahme.

a) Ergebnisse der Face Recognition Vendor Tests des NIST

Die Leistungsfähigkeit von Gesichtserkennungsalgorithmen kann am besten anhand unabhängiger Tests beurteilt werden, denn dadurch ist eine Vergleichbarkeit gewährleistet. Das US-amerikanische National Institute of Standards and Technology (NIST) führt regelmäßig die Face Recognition Vendor Tests durch, bei denen Gesichtserkennungsentwickler ihre Algorithmen evaluieren lassen können. Dabei zeigt sich mit jedem Test ein erheblicher und immer schnellerer Fortschritt in der Leistungsfähigkeit. Bereits in den Jahren 2013 bis 2018 wurden massive Genauigkeitssteigerungen erzielt; mindestens 30 Algorithmen übertrafen den genauesten

einer massiven Fahndung, der Schließung der 30.000-Einwohner-Stadt Watertown, Massachusetts, und zu einer tödlichen Konfrontation mit der Polizei führte. Damals war es den Strafverfolgungsbehörden nicht möglich, die beiden Verdächtigen per Gesichtserkennung zu identifizieren. Heute, zehn Jahre später, hat sich die Technologie jedoch so stark verbessert, dass die Täter womöglich hätten identifiziert werden können, ohne die Öffentlichkeit um Hilfe zu bitten und damit die Verdächtigen darauf aufmerksam zu machen, dass die Polizei ihnen auf der Spur war. Vielleicht hätte die heutige Gesichtserkennungstechnologie den Schusswechsel im öffentlichen Raum und den Tod eines Polizeibeamten verhindern können.

151 Zu diesem Trade-off auch *Grother/Ngan/Hanaoka*, Face Recognition Technology Evaluation (FRTE) Part 2: Identification, NISTIR 8271 Draft Supplement, 2023, 10, 32.

Algorithmus aus der vorherigen Testperiode (2010 bis 2013).[152] Der beste Gesichtserkennungsalgorithmus bei der letzten Evaluierung (Stand 2023; Algorithmus 2019/2020 eingereicht) ist nun noch einmal wesentlich genauer; seine Performance geht über alles hinaus, worüber der vorherige Test berichtet hatte.[153] Ihm wird eine „beinahe perfekte Erkennungsleistung"[154] bescheinigt.[155]

Dieser deutliche Fortschritt beruht auf dem zunehmenden Einsatz sog. Deep Convolutional Neural Networks (einer Form von künstlichen neuronalen Netzen).[156] Die dadurch entwickelten Algorithmen sind zunehmend toleranter gegenüber Fotos von geringer Qualität, mit schlechten Lichtverhältnissen oder auf denen die Person nicht direkt in die Kamera blickt. Viele Algorithmen sind mittlerweile sogar in der Lage, ein von der Seite aufgenommenes Gesicht korrekt einem Frontalfoto der Person zuzuordnen. Damit wurde ein lang ersehnter Meilenstein in der Gesichtserkennungsforschung erreicht.[157]

152 *Grother/Ngan/Hanaoka*, Face Recognition Technology Evaluation (FRTE) Part 2: Identification, NISTIR 8271 Draft Supplement, 2023, 8.

153 *Grother/Ngan/Hanaoka*, Face Recognition Technology Evaluation (FRTE) Part 2: Identification, NISTIR 8271 Draft Supplement, 2023, 8.

154 Abgeleitet wurde dies davon, dass der Algorithmus eine Rank one miss rate von 0,1 % erreichte. Die Rank one miss rate ist (neben z. B. der False acceptance rate und der False non-acceptance rate) eine weitere Möglichkeit, die Genauigkeit zu messen. Sie besteht darin, unabhängig vom Schwellenwert zu fragen, ob der Treffer mit dem höchsten Übereinstimmungswert (Ähnlichkeitswert) ein falscher Treffer ist, und daraus eine Rank one miss rate zu berechnen, also die Rate, bei der das Paar mit dem höchsten zurückgegebenen Ähnlichkeitswert (Rank one der Suchergebnisse) keine echte Übereinstimmung ist.

155 *Grother/Ngan/Hanaoka*, Face Recognition Technology Evaluation (FRTE) Part 2: Identification, NISTIR 8271 Draft Supplement, 2023, 8.

156 *Grother/Ngan/Hanaoka*, Face Recognition Technology Evaluation (FRTE) Part 2: Identification, NISTIR 8271 Draft Supplement, 2023, 8; siehe auch *Niederée/Nejdl* in Ebers/Heinze/Krügel/Steinrötter, Künstliche Intelligenz und Robotik, 2020, § 2 Technische Grundlagen der KI, Rn. 74 ff. In den vergangenen ein bis zwei Jahren werden zudem vermehrt Vision Transformer Modelle, eine andere Form von künstlichen neuronalen Netzen, verwendet.

157 *Grother/Ngan/Hanaoka*, Face Recognition Technology Evaluation (FRTE) Part 2: Identification, NISTIR 8271 Draft Supplement, 2023, 8.

b) Einordnung

Allerdings ordnet das NIST selbst diese Ergebnisse kritisch ein. Zunächst wurden diese sehr geringen Fehlerraten nur bei Tests mit gut beleuchteten polizeilichen Fotos (Mugshot images) erzielt, die in einem überwachten Setting aufgenommen wurden.[158] Bei einer Erkennung anhand von Bildern, die unter nicht-kontrollierten Umständen aufgenommen wurden (z. B. Webcam-Bilder von schlechterer Qualität), stieg die Fehlerrate selbst bei genaueren Algorithmen oft um über 20 %. Darüber hinaus variieren die Algorithmen enorm in ihrer Genauigkeit. So liegt beispielsweise die falsch-negative Fehlerquote des besten Algorithmus' in einem Szenario bei weit unter 1 %, die Fehlerquote des schlechtesten bei über 50 %.[159] Zudem spielt die Größe der Datenbank eine Rolle für die Fehlerraten; je mehr Personen sich in ihr befinden, desto wahrscheinlicher ist es, dass verschiedene Personen sich ähneln und daher ein falsches Match erzielt wird.[160] Fehler sind außerdem wahrscheinlicher, wenn ein großer Zeitabstand zwischen den Bildaufnahmen einer Person liegt.[161]

5. Höhere Fehlerraten bei einigen Bevölkerungsgruppen

Gesichtserkennungssysteme stehen in der Kritik, „verzerrt" („biased") zu sein, da sich das Problem der Fehl-Erkennungen ungleich auf verschiedene Bevölkerungsgruppen auswirkt. In einer eigens hierzu durchgeführten Studie hat das NIST 189 Gesichtserkennungsalgorithmen von 99 Entwicklern auf demografisch bedingte Unterschiede in der Genauigkeit getestet und kam zu dem Ergebnis, dass viele Gesichtserkennungssysteme People of Color, Frauen, Kinder und alte Menschen häufiger falsch als Treffer identifizieren als andere demografische Gruppen.[162] Die meisten Fehler

158 *Grother/Ngan/Hanaoka*, Face Recognition Technology Evaluation (FRTE) Part 2: Identification, NISTIR 8271 Draft Supplement, 2023, 8.

159 *Grother/Ngan/Hanaoka*, Face Recognition Technology Evaluation (FRTE) Part 2: Identification, NISTIR 8271 Draft Supplement, 2023, 9.

160 *Grother/Ngan/Hanaoka*, Face Recognition Technology Evaluation (FRTE) Part 2: Identification, NISTIR 8271 Draft Supplement, 2023, 10.

161 *Grother/Ngan/Hanaoka*, Face Recognition Technology Evaluation (FRTE) Part 2: Identification, NISTIR 8271 Draft Supplement, 2023, 10 f.

162 Umfassend hierzu *Grother/Ngan/Hanaoka*, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, 2019. Siehe auch bereits *Klare/Burge/Klontz/Vorder Bruegge/Jain*, IEEE Transactions on Information Forensics and Security 2012, 1789.

traten bei der Erkennung von weiblichen People of Color auf.[163] Bei vielen Algorithmen variierten die False acceptance rates über die verschiedenen Bevölkerungsgruppen hinweg um das 10- bis über 100-fache.[164] Solche Unterschiede in der Erkennungsgenauigkeit fand das NIST bei den meisten, aber nicht bei allen Algorithmen.[165] Bei Gesichtserkennungssystemen, die sich allgemein durch eine geringe Fehlerrate auszeichnen, ist tendenziell auch weniger mit gruppenbezogenen Unterschieden in den Fehlerraten zu rechnen.[166] Insgesamt bestanden jedoch große Unterschiede zwischen den verschiedenen Algorithmen mit Blick auf die Genauigkeit bei der Identifizierung verschiedener demografischer Gruppen.[167]

Bemerkenswert ist allerdings, dass viele in China trainierte Algorithmen nicht die erhöhten False acceptance rates für chinesische Gesichter aufwiesen, die in anderen Ländern entwickelte Algorithmen hatten.[168] Der NIST-Bericht kam daher zu dem Schluss, dass nicht-diverse Trainingsdaten der Grund für die Genauigkeitsunterschiede bei vielen Algorithmen sein könnten und dass Entwickler, die in vielfältigere Trainingsdaten investieren, diese demografischen Effekte abmildern könnten.[169] Daher wird vielfach geschlussfolgert, dass diese „Defekte" in Zukunft durch weitere Forschung

---

Vgl. auch den Hinweis in *Europäische Kommission*, Weißbuch „Zur künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen", COM(2020) 65 final, 2020, 13. Die in diesem Kontext sehr häufig zitierte Studie „Gender Shades" von Buolamwini und Gebru befasste sich nicht mit Gesichtserkennung, sondern mit Algorithmen zur Klassifizierung von Gesichtern; siehe *Buolamwini/Gebru*, Proceedings of Machine Learning Research 2018, 1, 9.

163 *Grother/Ngan/Hanaoka*, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, 2019, 3.

164 *Grother/Ngan/Hanaoka*, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, 2019, 2. Sie verwenden den Begriff „false positive rate" oder „false positive identification rate".

165 *Grother/Ngan/Hanaoka*, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, 2019, 3, 8.

166 *Grother/Ngan/Hanaoka*, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, 2019, 2.

167 *Grother/Ngan/Hanaoka*, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, 2019, 2.

168 *Grother/Ngan/Hanaoka*, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, 2019, 71.

169 *Grother/Ngan/Hanaoka*, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, 2019, 71. Siehe auch zuvor schon *Phillips/Jiang/Narvekar/Ayyad/O'Toole*, ACM Transactions on Applied Perception 2011, 1.

und umfangreichere, vielfältigere Datenbanken automatisierter Gesichtserkennung behoben würden.[170]

Zum jetzigen Zeitpunkt ist es jedoch eine Tatsache und Stand der Forschung, dass viele Algorithmen bei People of Color, Frauen, älteren Menschen und Kindern weniger genau sind.[171] Diese Gesichtserkennungsalgorithmen machen also nicht nur Fehler, sondern sie machen noch *mehr* Fehler, wenn es um diese Bevölkerungsgruppen geht, insofern sind sie ihnen gegenüber „voreingenommen" („biased").

Eine zusätzliche Ungleichheit in der Betroffenheit von Fehlidentifizierungen kann durch den Inhalt der Datenbank entstehen, die per Gesichtserkennung durchsucht werden. Personen mit bestimmten ethnischen Charakteristika werden häufiger von der Polizei kontrolliert (Racial Profiling[172]) und sind daher auch häufiger Beschuldigte in einem Ermittlungsverfahren.[173] Damit ist es auch wahrscheinlicher, dass sie erkennungsdienstlich behandelt und in eine polizeiliche Datenbank aufgenommen werden, die durchsucht wird, wodurch die Gefahr besteht, dass ihr Bild als (falschpositive) Übereinstimmung mit einem Verdächtigen angezeigt werden. Die

170 Siehe etwa *Law Journal Editorial Board*, Commentary, New Jersey Law Journal, 26.4.2020, https://perma.cc/EE9A-XPP9. Siehe zu technischen Möglichkeiten solches Verzerrungen zu verringern auch *Gong/Liu/Jain*, in: Li/Jain/Deng, Handbook of Face Recognition, 2024, 347.

171 Außerdem ist nicht klar, wie die Fairness mit Blick auf die Fehlerquoten bei Gesichtserkennung gemessen werden soll, für zwei verschiedene Ansätze siehe etwa *Howard/Laird/Sirotin/Rubin/Tipton/Vemury*, *Evaluating*, in: Rousseau/Kapralos, Pattern Recognition, Computer Vision, and Image Processing, 2023, 431.

172 Für eine Verfassungswidrigkeit des Racial Profiling etwa *Tischbirek/Wihl*, JZ 2013, 219.

173 Vgl. nur *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. Zu häufigeren Kontrollen und Festnahmen Schwarzer und Hispanics in den USA, selbst bei geringfügigen Vergehen, siehe *Heath*, USA TODAY v. 19.11.2014, https://perma.cc/5YQ8-T6WM; mit Blick auf stop-and-frisks *Goel/Rao/Shroff*, Annals of Applied Statistics, 2016, 365, 367 („[W]e find that blacks and Hispanics were disproportionately involved in low hit rate stops."); *Gelman/Fagan/Kiss*, Journal of the American Statistical Association 2007, 813, 821 („In the period for which we had data, the NYPD's records indicate that they were stopping blacks and Hispanics more often than whites, in comparison to both the populations of these groups and the best estimates of the rate of crimes committed by each group.").

Fehleranfälligkeit von Gesichtserkennung kann für Angehörige einer solchen Ethnie daher doppelt erhöht sein: dadurch, dass der Algorithmus weniger gut für ihre Ethnie funktioniert, und dadurch, dass sie in der durchsuchten Datenbank überproportional häufig vertreten sind.

6. Fazit

Automatisierte Gesichtserkennung ist nicht fehlerfrei. Die Technologie entwickelt sich jedoch rasant weiter; in den kommenden Jahren und Jahrzehnten werden die Fehl-Erkennungen immer weiter abnehmen. Ganz verschwinden werden die Fehler allerdings nicht. Gesichtserkennung wird nie perfekt funktionieren, da auch die zu durchsuchenden Bilder nicht immer perfekt sein werden. Schlechte Bildqualität, Aufnahmen aus schrägem Winkel und ungünstige Lichtverhältnisse werden weiterhin dazu führen, dass Personen auf einem Foto fälschlicherweise erkannt oder nicht erkannt werden. Im Blick zu behalten ist auch, dass viele Gesichtserkennungsalgorithmen für einige Bevölkerungsgruppen höhere Fehlerraten aufweisen.

Da jedoch auch Menschen bei der Gesichtserkennung keineswegs fehlerfrei sind,[174] ist die Frage der Zukunft aber nicht „Ist die Technologie fehlerfrei?". Die entscheidende Frage – die es noch zu erforschen gilt – wird vielmehr sein: „Macht die Technologie *weniger* Fehler als der Mensch?".

F. Einsatz in Deutschland

In Deutschland setzen BKA, Bundespolizei, Landeskriminalämter und Landespolizeibehörden automatisierte Gesichtserkennung ein, um unbekannte Verdächtige zu identifizieren. Am meisten bekannt ist über den Einsatz des Gesichtserkennungssystems GES beim BKA. Dort können die Bundespolizei, die Landeskriminalämter und die Landespolizeibehörden Anfragen stellen. Dieser Abschnitt gibt einen Überblick über die Abläufe bei den Recherchen im GES und erörtert, was darüber hinaus über den Einsatz von Gesichtserkennung durch Polizeibehörden bekannt ist.

174 Dazu Kapitel III. B. II. 2. a).

I. Gesichtserkennungssystem GES beim BKA

Beim BKA wird seit 2008 das Gesichtserkennungssystem GES eingesetzt, um Bilder unbekannter Tatverdächtiger mit den Lichtbildern im Informationssystem INPOL abzugleichen.[175] Im Jahr 2021 wurden in dem System über 90.000 Recherchen durchgeführt und insgesamt 4.990 Personen identifiziert.[176] Die Erkenntnisse werden vorrangig als Hinweise in Ermittlungsverfahren verwendet.[177]

1. Durchsuchbare Datenbank: INPOL-Z

Das polizeiliche Informationssystem INPOL[178] ist ein elektronischer Datenverbund zwischen Bund und Ländern und wird vom BKA betrieben.[179] Es besteht aus dem zentralen System INPOL-Z, das den zentralen Datenbestand enthält, sowie Teilnehmersystemen, mit denen alle Polizeibehörden von Bund und Ländern Daten abrufen oder einspeichern können.[180] Die Bilder aus dem Zentralbestand INPOL-Z werden in einem weiteren Schritt an das GES geschickt und recherchefähig gespeichert.[181] Gegenwärtig sind 6,7 Millionen Porträtaufnahmen zu rund 4,6 Millionen Personen gespeichert (Stand: 2023), die durchsucht werden können.[182] Grundsätzlich

175 Webseite des Bundeskriminalamts, Gesichtserkennung, https://perma.cc/NZ3K-B555. Die Nutzung erfolgt durch eine begrenzte Personenanzahl in der Abteilung Kriminalwissenschaften und Technik (KT) sowie dem Zentralen Informations- und Fahndungsdienst (ZI), siehe BT-Drs. 20/8495, 6 (Anlage 1a). Zum GES auch *Arzt*, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, G. Informationsverarbeitung im Polizei- und Strafverfahrensrecht, Rn. 1175.

176 BT-Drs. 20/895, 9.

177 Summary report of the project „Towards the European Level Exchange of Facial Images" (TELEFI) 2021, 169, https://perma.cc/T6NE-GTRV.

178 Das polizeiliche Informationssystem INPOL wurde 2003 durch das System INPOL-neu ersetzt, zu den Hintergründen siehe etwa *Petri/Kremer*, in: Lisken/Denninger, Handbuch des Polizeirechts, 7. Aufl. 2021, A. Geschichte der Polizei in Deutschland, Rn. 136. Die Bezeichnung INPOL ist aber weiterhin gebräuchlich.

179 § 29 Abs. 1 BKAG. Zu INPOL auch näher *Golla*, in: Dietrich/Fahrner/Gazeas/von Heintschel-Heinegg, Handbuch Sicherheits- und Staatsschutzrecht, § 30 Kooperative Informationsressourcen, 2022, Rn. 34 ff.

180 Kritisch zur Rechtsgrundlage *Arzt*, in: Lisken/Denninger, Handbuch des Polizeirechts, G. Informationsverarbeitung im Polizei- und Strafverfahrensrecht, 7. Aufl. 2021, Rn. 1200 f.

181 BT-Drs. 20/895, 9.

182 BT-Drs. 20/7864, 24; BT-Drs. 20/5781, 7.

sind die Personen mit Porträtfoto gespeichert (Blick in die Kamera, gute Beleuchtung); vereinzelt sind jedoch auch „uncontrolled images" aus Überwachungsvideos hinterlegt, wenn kein anderes Bild einer Person verfügbar ist.[183] Eine Suche in Datenbanken mit Führerschein-, Personalausweis- oder Passfotos wird nicht durchgeführt; technisch wäre sie möglich, allerdings nicht mit der gegenwärtigen Infrastruktur.[184] Auch private Anbieter wie *Clearview AI* oder *PimEyes*[185] werden, soweit ersichtlich, nicht verwendet.

Im durchsuchbaren Zentralbestand INPOL-Z befinden sich zum einen Lichtbilder von verdächtigten, festgenommenen, gesuchten und verurteilten Personen. Es finden sich zum anderen aber auch etwa Lichtbilder der Datei „Gewalttäter Sport".[186] Durchsuchbar sind zudem die Lichtbilder aller Asylsuchenden – unabhängig davon, ob sie eine Straftat begangen haben oder einer solchen verdächtig waren.[187] Die überwiegende Anzahl der Lichtbilder stammt nach Angaben der Bundesregierung aus polizeilichen erkennungsdienstlichen Maßnahmen sowie aus erkennungsdienstlichen Behandlungen im Asylkontext.[188] Insgesamt seien in INPOL-Z 3.564.613 nichtpolizeiliche und 3.091.694 polizeiliche Daten gespeichert.[189]

183 Summary report of the project „Towards the European Level Exchange of Facial Images" (TELEFI) 2021, 75, https://perma.cc/T6NE-GTRV.

184 Summary report of the project „Towards the European Level Exchange of Facial Images" (TELEFI) 2021, 74, https://perma.cc/T6NE-GTRV. In besonderen Ausnahmesituationen können Polizeibehörden jedoch Zugriff auf ein Bild einer solchen Datenbank erlangen, um die Identität eines Individuums anhand eines 1:1-Abgleichs zu überprüfen.

185 *Pimeyes* ist eine online frei verfügbare Gesichtserkennungssoftware, siehe die Webseite von *Pimeyes* https://pimeyes.com/en.

186 Die Datei „Gewalttäter Sport" ist eine separate Datenbank; zusätzlich sind diese Lichtbilder jedoch auch im Zentralbestand INPOL-Z gespeichert und durchsuchbar. Zur Datei „Gewalttäter Sport" ausführlich *Arzt*, in: Lisken/Denninger, Handbuch des Polizeirechts, G. Informationsverarbeitung im Polizei- und Strafverfahrensrecht, 7. Aufl. 2021, Rn. 1254 ff.

187 Vgl. Summary report of the project „Towards the European Level Exchange of Facial Images" (TELEFI) 2021, 75 und Appendix 3, https://perma.cc/T6NE-GTRV; siehe auch *Gewerkschaft der Polizei*, Pressemitteilung v. 4.12.2023, https://perma.cc/VV7H-RRCC. Die Lichtbilder der Asylsuchenden sind separat gespeichert („stored separately from the criminal database"), vgl. Summary report of the project „Towards the European Level Exchange of Facial Images" (TELEFI) 2021, Appendix 6, https://perma.cc/T6NE-GTRV.

188 Vgl. BT-Drs. 20/895, 9 („Die überwiegende Anzahl der Daten stammt aus polizeilichen erkennungsdienstlichen Maßnahmen sowie aus erkennungsdienstlichen Behandlungen im Asylkontext (Amtshilfeverfahren, vgl. §§ 16 Absatz 1, 19 Absatz 2 des Asylgesetzes (AsylG) oder § 49 Absatz 3 bis 9 des Aufenthaltsgesetzes (AufenthG)).").

2. Ablauf

Deutsche Polizeien können Bildmaterial eines unbekannten Tatverdächtigen mit den in INPOL-Z erfassten Lichtbildern abgleichen lassen.[190] Im GES werden jährlich zehntausende Suchläufe durchgeführt; Tendenz steigend.[191] Allein die Bundespolizei hat 2022 auf diese Weise rund 2.800 unbekannte Personen identifiziert.[192] Der Einsatz wird nicht beschränkt auf bestimmte (etwa besonders schwere) Straftaten.[193]

a) Bild eines Tatverdächtigen

Das Gesichtserkennungssystem wird als Unterstützungswerkzeug zur Personenidentifizierung eingesetzt und soll Ermittlungshinweise bei Fällen generieren, in denen lediglich Bilder eines unbekannten Tatverdächtigen vorliegen.[194] Hierzu übermittelt die Polizeibehörde zunächst das Untersuchungsmaterial (Foto der unbekannten Person) per FileShare-Link zum Download an die zuständige Stelle; dieses wird dann im GES hochgeladen. Häufig ist der Verdächtige nicht unmittelbar bei der Ausführung der Tat zu sehen, sondern beim Betreten oder Verlassen des Tatorts. Bewegtbilder

189 BT-Drs. 20/895, 9.

190 Siehe Summary report of the project „Towards the European Level Exchange of Facial Images" (TELEFI) 2021, 74 ff., https://perma.cc/T6NE-GTRV sowie die Webseite des Bundeskriminalamts, Gesichtserkennung, https://perma.cc/NZ3K-B555.

191 Webseite des Bundeskriminalamts, Gesichtserkennung, https://perma.cc/NZ3K-B555 („Aufgrund des steigenden Aufkommens digitaler Aufnahmen, z. B. in den sozialen Netzwerken und der durch Smartphones allzeitigen Möglichkeit Bilder zu fertigen, ist in den nächsten Jahren mit einem weiteren Anstieg der Zahl der GES-Recherchen zu rechnen.").

192 BT-Drs. 20/5781, 8.

193 So wurde Gesichtserkennung beispielsweise auch bei Beleidigung und einfacher Körperverletzung verwendet, um den Tatverdächtigen zu identifizieren, siehe das Beispiel in BT-Drs. 20/7995, 64 („Zunächst beleidigte UT [unbekannter Täter] einen Wahlkampfhelfer der AfD an einem Informationsstand anlässig [sic!] der anstehenden OB-Wahl mit den Worten ‚du Hurensohn' und spuckte ihm auf die Oberbekleidung, wodurch der GS [Geschädigte] ein starkes Ekelgefühl empfand. Weiterhin drohte er dem GS Schläge und die Verwüstung des Infostandes an. Ein Zeuge fertigte mittels Smartphone ein Bild des TV [Tatverdächtigen], wodurch dieser im Nachgang mittels Gesichtserkennung ermittelt werden konnte.").

194 Auch kann die Identität eines unbekannten Geschädigten ermittelt werden, BT-Drs. 20/8495, 6 (Anlage 1a).

(Videomaterial) können, soweit ersichtlich, nach aktuellem Stand im GES nicht direkt abgeglichen werden; hier müssen zuerst einzelne Standbilder extrahiert werden.[195] Die Suchbilder können aus polizeilichem Datenmaterial stammen, etwa aus Videoaufnahmen von staatlichen Überwachungskameras oder Bodycams. Die Bundespolizei identifiziert anhand von Überwachungsvideos an Bahnhöfen beispielsweise Straftaten im Bahnbereich wie Taschendiebstähle, Körperverletzung oder Exhibitionismus. Es können jedoch auch private Aufnahmen zum Abgleich herangezogen werden, angefertigt beispielsweise von Zeugen oder Überwachungskameras Privater (z. B. Supermärkte oder Banken). So wird Gesichtserkennung etwa genutzt, um Ladendiebstähle aufzuklären. Das Bayerische Landeskriminalamte gibt an, dass dort die Fotos in den meisten Fällen von Opfern oder Zeugen einer Straftat stammen; auch Bilder aus dem Internet oder Social Media würden immer häufiger verwendet.[196]

b) Generierung einer Kandidatenliste

Im nächsten Schritt generiert das GES eine Kandidatenliste,[197] typischerweise mit 10, 20 oder 100 Kandidaten.[198] In dieser werden die Personen nach dem Ähnlichkeitswert absteigend sortiert.[199] Unter besonderen Umständen besteht auch die Möglichkeit, die Liste auf 1000 Kandidaten zu erhöhen.[200] Bei dem Ähnlichkeitswert ist die Ähnlichkeit der den Gesichtern zugrunde liegenden Embeddings (also der biometrischen Merkmale) entscheidend, nicht die visuelle Ähnlichkeit des Aussehens.[201] Daher ist es möglich, dass ein Mann gesucht wird, auf Rang 1 der Ergebnisse sich jedoch eine Frau befindet;[202] beim GES besteht derzeit nicht die Möglichkeit,

195 BT-Drs. 18/11578, 9.
196 *Jordan*, Bayerischer Rundfunk v. 1.6.2021, https://perma.cc/7FQS-3WQS.
197 BT-Drs. 20/8495, 6 (Anlage 1a); vgl. auch *Werner*, Bayerns Polizei 2017, Heft 4, 24 („Ranking-Liste").
198 Summary report of the project „Towards the European Level Exchange of Facial Images" (TELEFI) 2021, 75, https://perma.cc/T6NE-GTRV. Derzeit ist die Erkennung grundsätzlich auf 100 Kandidaten voreingestellt.
199 BT-Drs. 20/8495, 6 (Anlage 1a).
200 Summary report of the project „Towards the European Level Exchange of Facial Images" (TELEFI) 2021, 75, https://perma.cc/T6NE-GTRV.
201 Vgl. auch *Werner*, Bayerns Polizei 2017, Heft 4, 24, („technisch" ähnliche Bilder).
202 Hierzu auch *Wimmer*, Süddeutsche Zeitung v. 16.1.2016, https://perma.cc/5AWG-M9DZ). Siehe für Fälle, in denen Gesichtserkennungssysteme eine Übereinstimmung

nach Geschlecht oder Ethnie zu filtern. Häufig werden sich die Personen, deren Embeddings ähnlich sind, jedoch ähnlich sehen. Der automatisierten Gesichtserkennung kommt daher eine entscheidende Filter- und Sortierfunktion zu.[203]

c) Überprüfung durch Experten

Diese Ergebnisse werden anschließend im 4-Augen-Vergleich von Menschen überprüft.[204] Dabei sind nur Sachverständige für Lichtbildvergleiche sowie Lichtbildexpertinnen und -experten mit der Identifizierung von Personen anhand von Bildern betraut. Die Sachverständigen haben hierfür eine mehrjährige Ausbildung und eine Prüfung absolviert,[205] die Lichtbildexpertinnen und -experten eine mehrwöchige Ausbildung und eine Prüfung.[206]

Die Experten erstellen entweder einen ausführlichen Untersuchungsbericht oder einen Kurzbericht. Im Rahmen eines Untersuchungsberichts[207] kann ein allgemeiner Vergleich (Überprüfung von Ähnlichkeiten und optischen Übereinstimmungen bzw. Abweichungen)[208] oder ein Detailvergleich (Feinstrukturen) durchgeführt werden. Voraussetzung für einen Detailver-

---

sehen, ein Mensch jedoch ohne Probleme erkennt, dass es sich um unterschiedliche Personen handelt, auch *Knoche/Rigoll,* 18th International Conference on Machine Vision and Applications 2023, arXiv, 1, 4.

203 *Schindler*, Biometrische Videoüberwachung, 2021, 203.

204 BT-Drs. 20/8495, 6 (Anlage 1a).

205 Zu der genauen Dauer existieren unterschiedliche Angaben, siehe etwa Webseite des Bundeskriminalamts, Gesichtserkennung, https://perma.cc/NZ3K-B555 (rund 4 Jahre); Summary report of the project „Towards the European Level Exchange of Facial Images" (TELEFI) 2021, 77, https://perma.cc/T6NE-GTRV (2,5 bis 3 Jahre); BT-Drs. 20/8495, 11 (Anlage 1a) (3 Jahre). Derzeit gibt es rund 70 solcher Sachverständigen für Lichtbildvergleiche.

206 Die Ausbildung dauert rund 11 Wochen und wird ebenfalls mit einer Prüfung abgeschlossen.

207 Bei dem Untersuchungsbericht handelt es sich nicht um ein durch einen Lichtbildsachverständigen angefertigtes Behördengutachten gem. § 256 StPO, sondern lediglich um die Erklärung der Behörde über den dienstlich durchgeführten Lichtbildvergleich eines sachverständigen Zeugen/Lichtbildexperten (§§ 85, 420 StPO).

208 Die Untersuchung erfolgt dabei anhand eines Vergleichs von individuellen anatomischen Grobstrukturen (allgemeiner Vergleich). Wenn eine Bewertung ausschließlich anhand von Grobstrukturen möglich ist, kann das Ergebnis der Untersuchung nur in folgende Bewertungskategorien eingeteilt werden: „Der Bildvergleich deutet auf eine Personenidentität hin.", „Personenidentität kann nicht ausgeschlossen werden.",

gleich und damit eine mögliche Identifizierung ist, dass die individuellen morphologischen Merkmale im Gesichts- bzw. Kopfbereich erkennbar und auswertbar sind. Daher muss das eingereichte Bildmaterial insbesondere von ausreichender Qualität sein. Die Bewertung der morphologischen Merkmale im Detailvergleich führt dann zu einer Wahrscheinlichkeitsaussage zur Identität (Übereinstimmung) der abgebildeten Personen, also ob sie „mit an Sicherheit grenzender Wahrscheinlichkeit", „mit hoher Wahrscheinlichkeit" oder „wahrscheinlich" identisch sind.[209]

Wenn hingegen die Qualität des eingereichten Bildes oder der Ausschnitt des Gesichts *nicht* ausreichend für einen Identitätsnachweis sind, dann wird lediglich ein Kurzbericht darüber erstellt, ob sich aufgrund augenscheinlicher Übereinstimmungen zumindest der „Verdacht" einer Personenidentität ergibt. Dies wird mit dem zusätzlichen Vermerk versehen, dass ein zweifelsfreier Identitätsnachweis mit dem vorliegenden Bildmaterial nicht zu führen sei und dass die Untersuchung lediglich eine „ermittlungsunterstützende Auswertung" darstelle. In dieser Konstellation sind Fehler, also Ermittlungen gegen einen Unbeteiligten, wahrscheinlicher. Damit ist nicht gemeint, dass die Experten einen *vorwerfbaren* Fehler machen; sie weisen schließlich darauf hin, dass aufgrund der schlechten Bildqualität eine eindeutige Identifizierung nicht möglich ist. Dennoch steht der Verdacht einer Personenidentität im Raum und gegen diese Person wird nun weiterermittelt.

d) Weitere Ermittlungsmaßnahmen

Insbesondere wenn die Recherche im Gesichtserkennungssystem wegen mangelnder Bildqualität oder mangelnder Erkennbarkeit der Gesichtszüge nur einen ermittlungsunterstützenden Hinweis in Form eines Verdachts der Personenidentität liefert, sind weitere Ermittlungen erforderlich. Gegen die Person, die potenziell der unbekannte Verdächtige auf dem eingereichten Bild ist, wird nun weiterermittelt, um herauszufinden, ob sie mit dem strafbaren Geschehen in Zusammenhang stand, etwa ob sie zur Tatzeit in der Nähe des Tatorts war. Der Untersuchungsbericht oder Kurzbericht wird in die Akte aufgenommen und ist bei Akteneinsicht für den Betroffenen

„Eine Aussage zur Personenidentität kann nicht getroffen werden.". Siehe hierzu auch KG, Urt. v. 15.12.2021 – 3 StE 2/20-1, BeckRS 2021, 47025 Rn. 99.

209 Vgl. auch KG Urt. v. 15.12.2021 – 3 StE 2/20-1, BeckRS 2021, 47025 Rn. 100.

einsehbar. Insgesamt werden Treffer des GES nicht als Beweismittel, sondern als Spurenansatz verwendet.

e) Case Study einer Recherche im GES

Zur besseren Anschaulichkeit wird im Folgenden ein fiktives Beispiel für eine Recherche im GES erläutert. Aus Gründen des Datenschutzes wurden Fotos der Autorin dieser Arbeit verwendet; bei den anderen Personen[210] handelt es sich um nicht real existierende Personen (Dummies).[211] Die oben dargestellten Schritte bei einer Recherche im GES können wie folgt ablaufen:

Bild einer Tatverdächtigen: Einem Geschädigten wird das Smartphone entwendet. Kurze Zeit später wird ein Bild einer Person mit dem Gerät aufgenommen und automatisch in die Cloud des Geschädigten übertragen. Auf dieses in der Cloud gespeicherte Foto kann der Geschädigte zugreifen und es den Strafverfolgungsbehörden übermitteln. Die aufgenommene Person steht im Verdacht, den Diebstahl oder eine Hehlerei (z. B. bei Kauf des Smartphones unter fraglichen Umständen) begangen zu haben.

Generierung einer Kandidatenliste: Ein Lichtbildsachverständiger oder -experte lädt das Foto der Verdächtigen im GES hoch. Im Rahmen der GES-Recherche wird dann eine Kandidatenliste generiert. Hier werden die Treffer angezeigt, die der Verdächtigen am ähnlichsten sehen (genauer: deren Embeddings dem Embedding der Verdächtigen am ähnlichsten sind). Wie bei GES-Recherchen üblich, ist in diesem Beispiel eingestellt, dass die ersten 100 Treffer angezeigt werden. Der Hintergrund von Abbildung 3 zeigt die Bildschirmansicht eines Monitors, so wie der Lichtbildsachverständige oder -experte sie nach jeder durchgeführten GES-Recherche sieht. Links befindet sich das Suchbild (das Bild der Verdächtigen). Rechts daneben befinden sich die im INPOL-Z eingestellten und im Rahmen der Suche getroffenen Frontalaufnahmen aus erkennungsdienstlichen Behandlungen, hier Trefferpositionen 1 bis 10.[212] Diese Seite kann mit jeweils zehn neu-

210 Treffer-Positionen 1, 3, 4, 5.

211 Für die Anfertigung dieser Abbildung bin ich Kay-Uwe Brandt, kriminaltechnischer Sachverständiger für Lichtbildvergleiche (Bundespolizeipräsidium, Referat 33 – Gesichtserkennung), zu großem Dank verpflichtet.

212 Auf Treffer-Position 2 befindet sich ein Foto der fiktiv in INPOL-Z eingestellten Autorin dieser Arbeit als mögliche Täterin.

en Aufnahmen aus erkennungsdienstlichen Behandlungen weitergeblättert werden.

Überprüfung durch Experten: Innerhalb der Benutzeroberfläche ist in dem Fenster im Vordergrund die Bildschirmansicht des zweiten Monitors dargestellt, auf dem ein Lichtbildsachverständiger oder -experte dann anhand einer vergleichenden Gegenüberstellung der sichtbaren morphologischen Merkmale im Gesicht und Halsbereich zwischen der Person auf dem Suchbild und der Person auf der Treffer-Aufnahme (hier: Position 2) über die Identität der Personen entscheidet.[213]

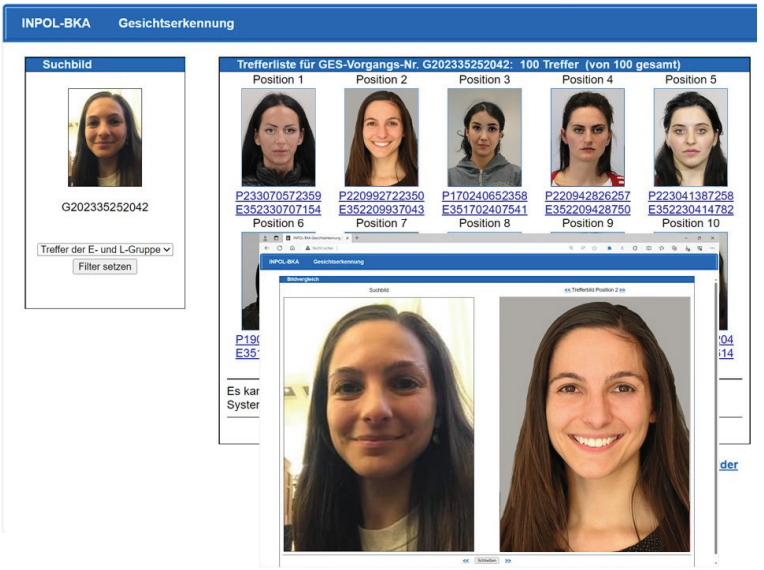

Abbildung 3: Fiktives Beispiel einer Recherche im GES

Ein Lichtbildsachverständiger oder -experte würde bei diesem Lichtbildvergleich zu dem Ergebnis kommen, dass es sich „mit hoher Wahrscheinlichkeit" um ein und dieselbe Person handelt.[214] Beim Vergleich würden

213 Auf dieser Seite können die Treffer-Gegenüberstellungen entweder mit den blauen „>>" um eine Position weiter- oder zurückgeschaltet oder durch Anklicken mit dem Mauszeiger eines anderen Trefferbildes auf Monitor 1 aktualisiert werden.

214 Persönliche Kommunikation mit Kay-Uwe Brandt, kriminaltechnischer Sachverständiger für Lichtbildvergleiche (Bundespolizeipräsidium, Referat 33 – Gesichtserkennung).

individualtypische Übereinstimmungen in den Grob- und Feinstrukturen festgestellt; Abweichungen sind nicht erkennbar.

Weitere Ermittlungsmaßnahmen: Es werden weitere Maßnahme getroffen, um zu ermitteln, ob es sich bei der abgebildeten Person um diejenige handelt, die den Diebstahl des Smartphones oder (z. B. durch Kauf des Smartphones unter fraglichen Umständen) eine Hehlerei begangen hat. Hier käme als Ermittlungsmaßnahme zunächst vor allem eine Ladung der Verdächtigen zur Vernehmung als Beschuldigte (§ 163a StPO) in Betracht.

3. Keine näheren Informationen über Trainingsprozess des GES

Das GES wurde bei dem deutschen Unternehmen *Cognitec* erworben[215] und basiert auf Methoden des maschinellen Lernens.[216] Nähere Informationen über die detaillierte Arbeitsweise der Komponenten und Details zu den Trainingsprozessen sind nicht bekannt,[217] da sie unter das Betriebsgeheimnis des Herstellers fallen.[218] Wie divers und ausgewogen die Trainingsdaten waren und ob (große) Unterschiede bei den Fehlerraten für verschiedene Bevölkerungsgruppen bestehen, ist nicht bekannt. Ab 2024 wird mit „GES-neu" ein neues Gesichtserkennungssystem zur Anwendung kommen; dessen Hersteller ist nicht öffentlich bekannt.

4. Keine Evaluierung der grundsätzlichen Leistungsfähigkeit des GES

Eine Evaluierung der grundsätzlichen Leistungsfähigkeit des Gesichtserkennungssystems erfolgt, soweit ersichtlich, nicht. Dies wird in einer Antwort der Bundesregierung auf eine Kleine Anfrage damit begründet, dass

215 Summary report of the project „Towards the European Level Exchange of Facial Images" (TELEFI) 2021, 75, https://perma.cc/T6NE-GTRV. Verwendet wird die Face VACS Software.

216 BT-Drs. 20/8495, 6 (Anlage 1a).

217 Eine Trefferrate des Systems wird nicht ermittelt. Dies wird damit begründet, dass die schlussendliche Auswahl und Identifizierung durch Menschen erfolgt, vgl. Summary report of the project „Towards the European Level Exchange of Facial Images" (TELEFI) 2021, 76, https://perma.cc/T6NE-GTRV. Dies erklärt jedoch nicht, warum nicht beispielsweise berechnet und anschließend berichtet werden könnte, in wie viel Prozent der Fälle der Gesuchte zwar in der Liste enthalten war, aber auf einem sehr niedrigen Rang.

218 BT-Drs. 20/8495, 6 (Anlage 1a).

dies „nur sehr bedingt möglich [sei], da die zur Verfügung stehende Datenbasis nur begrenzt geeignet ist".[219] Auch werde „faktisch jedes Ergebnis evaluiert bzw. verifiziert", da menschliche Experten die letztendliche Identifizierung anhand der Kandidatenliste vornehmen.[220] Eine Veröffentlichung von Evaluierungsergebnissen erfolge daher nicht.[221]

5. Keine Evaluierung der auf GES-Recherchen basierenden Ermittlungsverfahren

Soweit ersichtlich wird auch nicht evaluiert, in wie vielen Fällen es sich bei den Personen, auf die nach der menschlichen Überprüfung ein Verdacht fällt, tatsächlich um den gesuchten unbekannten Täter handelte. Ebenfalls wird nicht systematisch nachverfolgt und ausgewertet, wie häufig und welche Ermittlungsmaßnahmen gegen Unbeteiligte durchgeführt werden, weil sie ursprünglich per Gesichtserkennung (fälschlicherweise) identifiziert wurden.

II. Landeskriminalämter und Landespolizeibehörden

Bei den Landeskriminalämtern sind Schnittstellen zum GES eingerichtet. Zudem betreiben das Landeskriminalamt Bayern und einige Landespolizeibehörden eigene Gesichtserkennungssysteme.

1. Schnittstellen zum GES bei den Landeskriminalämtern

Bei den Landeskriminalämtern sind Schnittstellen zum GES eingerichtet; sie können daher Lichtbilder in das System einlesen und selbstständig im Lichtbildbestand des INPOL-Z recherchieren.[222] Auch hier sind nur ausgebildete Lichtbildexpertinnen und -experten oder Lichtbildsachverständige

219 BT-Drs. 20/8495, 18 (Anlage 1a).
220 BT-Drs. 20/8495, 18 (Anlage 1a).
221 Vgl. BT-Drs. 20/8495, 18 (Anlage 1a) (Spalte 6 Veröffentlichung: „Nein").
222 Siehe zur Schnittstelle des LKA Bayern *Frankl*, Kriminalistik 2019, 130, 131 und *Werner*, Bayerns Polizei 2017, Heft 4, 24 sowie zur Schnittstelle des LKA Rheinland-Pfalz D*er Landesbeauftragte für den Datenschutz Rheinland-Pfalz*, 22. Tätigkeitsbericht 2008-2009, LT-Drs. RP 15/4300, 2010, 69 f.

mit der Überprüfung der Kandidatenliste betraut und es wird ebenfalls ein 4-Augen-Vergleich vorgenommen.[223] Die mit der Erkennung befassten Beamten sind nicht zugleich für die Ermittlungen in diesem Fall verantwortlich.[224] Sie kennen die groben Umstände, etwa welches Delikt im Raum steht, aber keine näheren Details (z. B. wer der Geschädigte ist).[225] Das Bayerische Landeskriminalamts gibt an, die Palette der Delikte reiche „von der Beleidigung, dem Betrug, dem klassischen Ladendiebstahl über die Vergewaltigung, dem Raubüberfall bis zum Mord".[226] Auch nach Schlägereien, bei Drogendelikten und im Bereich der Kinderpornografie wird Gesichtserkennung verwendet, um unbekannte Verdächtige zu identifizieren.[227] Schwere Delikte seien allerdings „zahlenmäßig nicht so häufig vertreten".[228] Einige Polizeipräsidien haben ebenfalls direkten Zugriff auf das GES.[229] Eine systematische Auswertung der Ermittlungserfolge und Ermittlungen gegen Unbeteiligte nach GES-Recherchen erfolgt auch hier, soweit ersichtlich, nicht.

2. Eigene Systeme beim LKA Bayern und anderen Landespolizeibehörden

Das Bayerische Landeskriminalamt betreibt zudem ein eigenes Gesichtserkennungssystem mit eigener Datenbank. In dieser sollen noch andere Bilder als in INPOL-Z gespeichert sein, etwa nicht nur bereits erkennungsdienstlich behandelte Personen, sondern auch Bilder von unbekannten Verdächtigen.[230] Zudem verwenden einige Landespolizeibehörden ein eigenes

223 *Frankl*, Kriminalistik 2019, 130, 131; *Werner*, Bayerns Polizei 2017, Heft 4, 24.

224 Deutschlandfunk, Podcast KI Verstehen, Gesichtserkennung, 2.11.2023, https://www.deutschlandfunk.de/gesichtserkennung-macht-ki-uns-zu-glaesernen-buergern-dlf-f5b06014-100.html.

225 Deutschlandfunk, Podcast KI Verstehen, Gesichtserkennung, 2.11.2023, https://www.deutschlandfunk.de/gesichtserkennung-macht-ki-uns-zu-glaesernen-buergern-dlf-f5b06014-100.html.

226 *Jordan*, Bayerischer Rundfunk v. 1.6.2021, https://perma.cc/7FQS-3WQS.

227 *Schmidt*, Süddeutsche Zeitung v. 4.5.2018 https://perma.cc/WAB6-F4EW; *Wimmer*, Süddeutsche Zeitung v. 16.1.2016, https://perma.cc/5AWG-M9DZ.

228 *Jordan*, Bayerischer Rundfunk v. 1.6.2021, https://perma.cc/7FQS-3WQS.

229 Siehe nur LT-Drs. Bremen 20/1074, 5; *Kerber*, Der Guller v. 26.8.2023, https://perma.cc/WC3P-8QSM.

230 Vgl. bereits 2018, *Schmidt*, Süddeutsche Zeitung v. 4.5.2018 https://perma.cc/WAB6-F4EW: „In der Datenbank des Bundeskriminalamts sind nur Verbrecher erfasst, die bereits erkennungsdienstlich behandelt wurden. Egger will noch in diesem Jahr beim LKA eine neue Datenbank aufbauen mit Bildern von unbekannten Verdäch-

Gesichtserkennungssystem, um ihren lokalen Lichtbildbestand zu durchsuchen.[231] Hierüber ist nichts Näheres öffentlich bekannt.

III. Einordnung

Zur Einordnung ist noch ein kritischer Hinweis geboten. Die Erläuterungen in diesem Abschnitt dürfen nicht darüber hinwegtäuschen, dass die oben genannten Informationen weit verstreut und daher für die Öffentlichkeit kaum nachvollziehbar sind. Auch gibt es beispielsweise keine Übersicht dazu, welche Polizeibehörden Gesichtserkennung verwenden und vor allem, welche von ihnen ein eigenes Gesichtserkennungssystem einsetzen und auf welche Weise. Die Anfragen an die Bundesregierung, aus denen viele der Informationen stammen, betreffen naturgemäß immer nur die Verwendung von Gesichtserkennung durch Bundespolizeibehörden; Anfragen auf Landesebene gibt es über Gesichtserkennung kaum. Mindestens missverständlich ist zudem, dass das BKA auf seiner Webseite angibt, es würde zur Gesichtserkennung das Bild eines Unbekannten mit Lichtbildern von „Straftätern" abgeglichen, ohne zu erwähnen, dass sich unter den durchsuchten Bildern auch alle Asylsuchenden befinden sowie zahlreiche Personen, die lediglich einmal einer Straftat *verdächtig* waren (und womöglich sogar freigesprochen wurden)[232].

---

tigen. Schlagen dieselben Täter mehrmals zu, könnte die Software dabei helfen, verschiedene Verbrechen einer einzelnen Person zuzuordnen. Das wiederum könnte die Ermittlungen erleichtern, wenn sich zuvor isolierte Spuren zu einem einzelnen Puzzle zusammenfügen. Zudem will [der Leiter der Abteilung Cybercrime beim bayerischen Landeskriminalamt] Egger in diesem Jahr „personell aufstocken" und „eine eigene Organisationseinheit" für die Bilderkennung schaffen".

231 Summary report of the project „Towards the European Level Exchange of Facial Images" (TELEFI) 2021, 75, https://perma.cc/T6NE-GTRV.

232 Deren Bilder können unter Umständen dennoch in einer erkennungsdienstlichen Datenbank gespeichert bleiben, dazu näher Kapitel II. A. I. 2. b) bb).

G. Chancen und Risiken des Einsatzes

"But I don't want comfort. I want God, I want poetry, I want real danger, I want freedom, I want goodness. I want sin."
– Aldous Huxley[233]

Als mächtige Strafverfolgungstechnologie birgt automatisierte Gesichtserkennung das Potenzial, abweichendes Verhalten schnell, effektiv und flächendeckend aufzuspüren und zu ahnden.

Was dabei auf der Strecke bleiben kann und welche Risiken der nachlässige oder gar missbräuchliche[234] Umgang mit sich bringt, zeigt ein Blick auf die Erfahrungen anderer Staaten, in denen bereits länger und umfassender automatisierte Gesichtserkennung in der Strafverfolgung verwendet wird.

Dieser Abschnitt gibt zunächst einen Überblick über die Möglichkeiten und Chancen, die automatisierte Gesichtserkennung bietet. Dann wird auf die Risiken eingegangen; hierfür werden Beispiele problematischen Umgangs mit der Technologie aus den USA, China und Russland beleuchtet.

I. Potenzial für die Strafverfolgung

Für eine effektive Strafverfolgung bietet automatisierte Gesichtserkennungstechnologie großes Potenzial und eine Reihe an Vorteilen, auch und gerade im Vergleich zu anderen Ermittlungstools und anderen biometrischen Identifizierungsmethoden. Die Technologie wird für die Polizeibehörden immer wichtiger; der Leiter der Abteilung Cybercrime beim bayerischen Landeskriminalamt prophezeit, dass die Gesichtserkennung für die Polizeiarbeit bald so wichtig sein wird wie Fingerabdrücke oder DNA-Spuren.[235]

---

233 *Huxley*, Brave New World, 1950, 197.

234 Auch bei korrektem und verantwortungsbewusstem Einsatz von Gesichtserkennung werden sich Fehler nie vollständig vermeiden lassen, da Gesichtserkennung nie fehlerfrei sein wird (hierzu Kapitel I. E. IV.) und da die menschlichen Fähigkeiten zur Überprüfung von Gesichtserkennungstreffern begrenzt sind (hierzu Kapitel III. B. II. 2. a)).

235 *Jordan*, Bayerischer Rundfunk v. 1.6.2021, https://perma.cc/7FQS-3WQS; siehe bereits 2018 *Schmidt*, Süddeutsche Zeitung v. 4.5.2018 https://perma.cc/WAB6-F4EW.

1. Effizienz

Mit Gesichtserkennung können große Lichtbildbestände wie polizeiliche Datenbanken deutlich schneller durchsucht werden. Viele Polizeibehörden setzen zur Erkennung von Verdächtigen zwar auch sogenannte Super Recognizer ein.[236] Diese Menschen haben eine weit überdurchschnittliche Fähigkeit zur Gesichtserkennung; sie können sich Gesichter einprägen und diese selbst nach Jahren wiedererkennen.[237] Doch selbst wenn diese in Höchstform in einer Viertelstunde durch tausend Fotos scrollen können, die Maschine ist schneller (und wird nicht müde).[238] Zudem können die menschlichen Super Recognizer nur Menschen wiedererkennen, die sie bereits einmal gesehen haben; die Technologie kann eine ganze Datenbank mit Millionen von Gesichtern scannen. Im Übrigen verfügen nur sehr wenige Menschen, etwa 2 % der Bevölkerung, über diese weit überdurchschnittliche Fähigkeit zur Gesichtserkennung.[239]

2. Einfache Erfassung und Verfügbarkeit von Gesichtsbildern

Gegenüber anderen biometrischen Identifizierungsmethoden hat die Gesichtserkennung einige entscheidende Vorteile. Für eine Identitätsermittlung anhand des Gesichts muss der Verdächtige nicht ergriffen werden, nicht kooperieren, er muss nicht einmal von der Aufzeichnung seines Gesichts und dem Abgleich per Gesichtserkennung wissen.[240] Da Aufnahmen von Gesichtern selbst aus großer Entfernung noch eine gute Auflösung haben können,[241] kann ein einziges Bild einer Überwachungskamera oder auf dem Smartphone eines Zeugen die Identifizierung ermöglichen. Dage-

236 Siehe nur für die Polizei München, *Rampe*, ZEIT Online v. 24.10.2023, https://perma.cc/BFK8-7VRU.

237 Zum, soweit ersichtlich, ersten wissenschaftlichen Test dieser Fähigkeit siehe *Russell/Duchaine/Nakayama*, Psychonomic Bulletin & Review 2009, 252.

238 In *Rampe*, ZEIT Online v. 24.10.2023, https://perma.cc/BFK8-7VRU spricht ein Super Recognizer davon, dass die softwarebasierte Gesichtserkennung bereits „unverzichtbar" sei, weil sie zuverlässig Gesichter aussortiere, die nicht gesucht sind.

239 *Russell/Duchaine/Nakayama*, Psychonomic Bulletin & Review 2009, 252 mwN.

240 Vgl. auch *Wei/Li*, in: Tistarelli/Champod, Handbook of Biometrics for Forensic Science, 2017, 177, 177 f. Zur hohen Erfassbarkeit („collectibility") des Gesichts bereits *Jain/Bolle/Pankanti*, in: Jain/Bolle/Pankanti, Biometrics, 1999, 1, 16.

241 Siehe nur *Wei/Li*, in: Tistarelli/Champod, Handbook of Biometrics for Forensic Science, 2017, 177.

gen kann ein Unbekannter anhand seiner Fingerabdrücke nur identifiziert werden, wenn er solche am Tatort hinterlassen hat. Die meisten anderen biometrischen Identifizierungsmethoden funktionieren zudem nur mit Kooperation des Betroffenen zuverlässig; für eine Retina- oder Iriserkennung beispielsweise muss er aus der Nähe und bei guten Lichtverhältnissen direkt in die Kamera blicken.[242]

Auch die einfache Verfügbarkeit von Gesichtsbildern ist ein großer Vorteil der Gesichtserkennung. Das gilt zum einen für die Aufnahmen von unbekannten Verdächtigen, die etwa bei der Tat oder beim Betreten oder Verlassen des Tatorts zu sehen sind. Immer mehr staatliche und private Überwachungskameras sind rund um die Uhr im Einsatz, um das Geschehen aufzuzeichnen – auch Raubüberfälle, Diebstähle und Gewalttaten; Smartphones machen es möglich, Schlägereien oder Tierquälerei zu filmen; in sozialen Medien können die Aufnahmen verbreitet werden.[243]

Gesichtsbilder zum Abgleich sind ebenfalls einfach verfügbar. Andere biometrische Fernidentifizierungsmethoden wie die Gangerkennung (Gait recognition) ermöglichen zwar auch eine Identifizierung aus der Ferne;[244] dann muss aber ein Gangprofil zu der entsprechenden Person in einer Datenbank gespeichert sein, mit der abgeglichen wird. Gesichtsbilder hingegen sind bereits vorhanden, etwa in polizeilichen Datenbanken oder

242 Wie bereits erwähnt, befindet sich die Retina (Netzhaut) am hinteren Teil des Auges und kann nur aus der Entfernung weniger Zentimeter gescannt werden; die Person muss zudem ihren Kopf für etwa 10–30 Sekunden stillhalten (zur Retina-Erkennung siehe nur *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). Iriserkennungen waren ursprünglich nur aus einer Entfernung von weniger als einem Meter und mit Kooperation des Betroffenen zuverlässig möglich. Zwar wird in den letzten Jahren vermehrt daran geforscht, eine höhere Genauigkeit zu erreichen, auch für die Erkennung aus mehreren Metern Entfernung und/oder in nicht kontrollierten Settings (unconstrained environments), bei denen die Betroffenen sich bewegen oder nicht direkt in die Kamera blicken, siehe nur *Nguyen/Fookes/Jillela/Sridharan/Ross*, Pattern Recognition 2017, 123; *Tistarelli/Champod*, in: Tistarelli/Champod, Handbook of Biometrics for Forensic Science, 2017, 1, 4. Die Genauigkeit solcher Iriserkennungen liegt dennoch weit hinter denen einer Gesichtserkennung.

243 Siehe auch die Webseite des Bundeskriminalamts, Gesichtserkennung, https://perma.cc/NZ3K-B555: „Aufgrund des steigenden Aufkommens digitaler Aufnahmen, z. B. in den sozialen Netzwerken und der durch Smartphones allzeitigen Möglichkeit Bilder zu fertigen, ist in den nächsten Jahren mit einem weiteren Anstieg der Zahl der GES-Recherchen zu rechnen."

244 Zur Gangerkennung siehe etwa *Makihara/Matovski/Nixon/Carter/Yagi*, Wiley Encyclopedia of Electrical and Electronics Engineering, 2015, 1.

anderen staatlichen Lichtbildsammlungen (z. B. Personalausweis- und Führerscheinfotos). Anwendungen wie *Clearview AI*[245] oder *PimEyes*[246] ermöglichen zudem mit wenigen Klicks eine Identifizierung anhand von Fotos von Social-Media-Plattformen und allgemein aus dem Internet.

3. Gesichtserkennung als einziger Spurenansatz

In vielen Fällen ist das Gesicht und damit die Gesichtserkennung der einzige Spurenansatz, um den Täter überhaupt ausfindig machen zu können. Von zwei solchen Beispielen berichtet der Leiter der Abteilung Cybercrime beim bayerischen Landeskriminalamt.[247]

Wird etwa ein Drogenkonsument festgenommen und befragt, so kennt er häufig den echten Namen seines Händlers nicht, hat aber seinen WhatsApp-Kontakt und damit auch dessen Profilfoto, teilweise mit dem (echten) Gesicht. Per Gesichtserkennung können die Strafverfolgungsbehörden dieses dann einfach mit einer polizeilichen Datenbank abgleichen und so den Namen des Drogenhändlers herausfinden, wenn er zuvor bereits erkennungsdienstlich behandelt wurde.

Auch bei körperlichen Auseinandersetzungen unter Personen, die sich nicht persönlich kennen, ist die Identifizierung der Täter ohne Gesichtserkennung kaum möglich. Der Leiter der Abteilung Cybercrime beim bayerischen Landeskriminalamt berichtet etwa von einem Fall der Körperverletzung in einer Münchner Diskothek.[248] Das Opfer kannte den Täter nicht, sodass keinerlei Ermittlungsansätze bestanden. Der Nachtclub hatte jedoch Fotos von der Party machen lassen und diese auf der Webseite veröffentlicht; auf zwei Bildern erkannte das Opfer den Angreifer. Mithilfe von Gesichtserkennung konnte der Fall gelöst werden: Der Täter war wegen eines früheren Vergehens bereits in der Datenbank erfasst und konnte so identifiziert werden.

245 Siehe Kapitel I. C. II. 1.
246 Die Gesichtserkennungssoftware von *Pimeyes* ist online frei verfügbar, siehe die Webseite von *Pimeyes*, https://pimeyes.com/en.
247 *Schmidt*, Süddeutsche Zeitung v. 4.5.2018 https://perma.cc/WAB6-F4EW.
248 *Schmidt*, Süddeutsche Zeitung v. 4.5.2018, https://perma.cc/WAB6-F4EW.

4. Überprüfbarkeit durch Menschen

Gesichtserkennung hat zudem den Vorteil, dass die Ergebnisse durch Menschen überprüft werden können. Die Vorschläge anderer KI-basierter Anwendungen in Strafverfolgung und Gefahrenabwehr (z. B. Algorithmen zur Rückfallprognose und Predictive Policing Systeme) können hingegen von Menschen häufig nicht nachvollzogen werden.[249] Zwar ist aufgrund der Komplexität der Rechenoperationen selbst für Entwickler von Gesichtserkennungsalgorithmen nicht nachvollziehbar, wie genau die Embeddings (numerische Darstellungen der Gesichtsmerkmale) zustande kommen.[250] Das Ergebnis ist jedoch grundsätzlich einer Überprüfung zugänglich, indem Menschen selbst die Merkmale der Gesichter (nicht der Embeddings) vergleichen können.[251] Die relevanten Merkmale (z. B. Hautunebenheiten, Narben etc.) können Sachverständige in schwierigeren Fällen dann einkreisen oder mit Pfeilen versehen; dadurch können auch Laien den Vergleich nachvollziehen.

Die grundsätzliche Überprüfbarkeit von Gesichtserkennungstreffern wird in Zukunft jedoch immer mehr in Frage gestellt werden. Dies gilt vor allem dann, wenn Gesichtserkennungsalgorithmen den Menschen in seiner Fähigkeit, Gesichter zu erkennen, übertreffen (teilweise ist dies bereits der Fall)[252]. Die Technologie kann dann zum Beispiel (korrekte) Übereinstimmungen selbst dann finden, wenn große Teile des Gesichts verdeckt sind und ein Mensch nicht mehr in der Lage wäre, zu erkennen und zu erklären, warum es sich um dieselbe Person handelt.

249 Zu dieser Problematik beim personenbezogenen Predictive Policing siehe etwa *Sommerer*, Personenbezogenes Predictive Policing, 2020, 142 („Wie genau das neue Datum bei einem PPP-Prozess zustande gekommen ist, ist für den Beamten vor Ort jedoch nicht unmittelbar nachvollziehbar, da Predictive Policing gerade dann eingesetzt wird, wenn statistische Berechnungen durchgeführt werden sollen, zu denen ein Beamter vor Ort nicht in der Lage wäre."). Vgl. auch *Rademacher/Perkowski*, JuS 2020, 713, 720.

250 Kapitel I. E. III.

251 Zu Fällen, in denen falsche Treffer der Maschine für einen Menschen sehr leicht zu erkennen sind („edge cases") *Knoche/Rigoll,* 18th International Conference on Machine Vision and Applications 2023, arXiv, 1, 4.

252 Vgl. in diese Richtung etwa bereits die Untersuchung von *Ramsthaler/Federspiel/Huckenbeck/Kettner/Lux/Verhoff*, Archiv für Kriminologie 2024, Band 254, 1.

II. Risiken

Um zu verstehen, welche Gefahren Gesichtserkennung mit sich bringen kann, lohnt sich ein Blick auf die Erfahrungen anderer Staaten, die diese Technologie schon länger und umfassender einsetzen als deutsche Strafverfolgungsbehörden. Anschließend wird auch darauf eingegangen, inwiefern diese Risiken für Deutschland relevant sind.

1. Erfahrung aus anderen Staaten

Weltweit setzen Strafverfolgungsbehörden mittlerweile auf Gesichtserkennung. Ein umfassendes Bild zu erhalten ist allerdings schwer möglich, da selbst in Ländern wie den USA, die bereits auf langjährige Erfahrungen mit Gesichtserkennung zurückblicken können, die Verwendung der Technologie häufig verdeckt bleibt.[253]

a) USA

Der Einsatz automatisierter Gesichtserkennung ist in den USA bereits weit verbreitet: Mindestens jede vierte Polizeibehörde verwendet die Technologie, um Verdächtige zu identifizieren;[254] die Hälfte der erwachsenen US-Amerikaner – über 117 Millionen Menschen – sind in Gesichtserkennungsdatenbanken gespeichert.[255] Dabei können die Strafverfolgungsbehörden nicht nur auf polizeiliche Datenbanken zurückgreifen, sondern häufig etwa auch Führerscheinfotos durchsuchen.[256]

253 *Karaboga/Frei/Ebbers/Rovelli/Friedewald/Runge*, Automatisierte Erkennung von Stimme, Sprache und Gesicht: Technische, rechtliche und gesellschaftliche Herausforderungen, 2022, 108, auch mit dem zutreffenden Hinweis, dass etwa der verbreitete Einsatz von *Clearview AI* erst im Rahmen eines Interviews mit dem CEO des Unternehmens bekannt wurde.

254 *Garvie/Bedoya/Frankle*, The Perpetual Line-Up: Unregulated Police Face Recognition in America, Center on Privacy & Technology, Georgetown Law, 2016, https://perma.cc/BSF9-9A9C; vermutlich sind die Zahlen seit diesem Report aus dem Jahr 2016 noch erheblich angestiegen.

255 *Garvie/Bedoya/Frankle*, The Perpetual Line-Up: Unregulated Police Face Recognition in America, Center on Privacy & Technology, Georgetown Law, 2016, https://perma.cc/BSF9-9A9C.

256 Siehe nur *Harwell*, The Washington Post v. 7.7.2019, https://perma.cc/74E9-MJ4R.

In vielen Bundesstaaten gibt es sowohl eine spezielle Einheit für die Durchführung von Gesichtserkennungssuchen in landesweiten Datenbanken als auch die Möglichkeit für Polizeibehörden, ihre eigene Gesichtserkennungssoftware zu erwerben, um dann (nur) die eigene Lichtbilddatenbank dieser Behörde zu durchsuchen. In Michigan beispielsweise enthält das Statewide Network of Agency Photos (SNAP) Lichtbilder von Festgenommenen, Lichtbilder der Strafvollzugsbehörde Michigan Department of Corrections und Lichtbilder des Michigan Department of State (einschließlich Bilder von Führerscheinen).[257] Polizeibehörden im Bundesstaat Michigan sowie auf Bundesebene können bei der SNAP-Einheit der Michigan State Police einen Antrag auf eine Gesichtserkennungsabfrage stellen, die daraufhin von einem geschulten Gesichtsprüfer in ihrem Namen durchgeführt wird. Das System liefert dann in der Regel eine Liste von Gesichtsbildern, die nach der vom System ermittelten Ähnlichkeit geordnet sind, zusammen mit dem Ähnlichkeitswert.[258] Ein geschulter Gesichtsprüfer vergleicht schließlich das Bild des unbekannten Verdächtigen manuell mit den von der Software zurückgegebenen Übereinstimmungen und entscheidet, ob eine der Personen dem unbekannten Verdächtigen ähnlich genug ist, um mit den Ermittlungen fortzufahren. Die Generierung der Gesichtserkennungsübereinstimmungen ist daher nur der erste Schritt, ein Mensch muss sie anschließend überprüfen. Polizeibehörden können auch Zugang zum SNAP-Desktop-Tool für Gesichtserkennung beantragen, um ihre eigenen Recherchen durchzuführen.[259] In diesen Fällen sind die Abfragen jedoch auf die Datenbank der Fahndungsfotos und Festgenommenen beschränkt. Die Polizei des Bundesstaates Michigan „empfiehlt" zwar, dass alle Gesichtserkennungsabfragen von Personal durchgeführt werden, das für den Vergleich und die Identifizierung von Gesichtern geschult ist,[260] eine verbindliche Regelung existiert aber nicht.

257 Michigan State Police, Facial Recognition – Frequently Asked Questions, https://perma.cc/7CNC-BRVR.

258 Michigan State Police, Facial Recognition – Frequently Asked Questions, https://perma.cc/7CNC-BRVR; vgl. auch *Grother/Ngan/Hanaoka*, Face Recognition Technology Evaluation (FRTE) Part 2: Identification, NISTIR 8271 Draft Supplement, 2023, 10.

259 Darüber hinaus können Polizeibehörden ein Live-Foto mit einer mobilen Gesichtserkennungslösung der Michigan State Police durchsuchen, Michigan State Police, Facial Recognition – Frequently Asked Questions, https://perma.cc/7CNC-BRVR.

260 Michigan State Police, Facial Recognition – Frequently Asked Questions, https://perma.cc/7CNC-BRVR.

Viele Strafverfolgungsbehörden in den USA verwenden zudem *Clearview AI*, um Verdächtige zu identifizieren. Über *Clearview AI* kann jedes öffentlich gepostete Foto gefunden werden – auch wenn die Person ihr Social Media Profil inzwischen auf privat gestellt hat oder nicht selbst, sondern eine dritte Person das Foto hochgeladen hat. Mehrere US-Strafverfolgungsbehörden nutzen die Software bereits regelmäßig, um Verdächtige zu identifizieren.[261] Nach dem Sturm auf das Kapitol identifizierte das FBI beispielsweise einen Verdächtigen, der selbst keine sozialen Medien nutzte, aber auf einem alten Instagram-Foto seiner Freundin zu sehen war.[262] Die Polizei hat *Clearview AI* auch eingesetzt, um Verdächtige zu identifizieren, die bei Protesten Polizisten angegriffen haben sollen.[263]

Der Einsatz von Gesichtserkennung steht in den USA vor allem deshalb stark in der Kritik, weil bereits sechs Fälle bekannt geworden sind, in denen gänzlich Unbeteiligte nach einem falschen Gesichtserkennungstreffer festgenommen wurden und mehrere Tage in Haft verbrachten.[264] In allen Fällen waren die Betroffenen Schwarze.

Bislang fehlt es an einer nationalen gesetzlichen Regelung des Einsatzes automatisierter Gesichtserkennung in den USA. Die Rechtslage in den einzelnen Bundesstaaten und Städten ist uneinheitlich. Während der Einsatz an vielen Orten zugelassen, aber näher geregelt wird, erließ etwa der Bundesstaat Massachusetts ein Moratorium;[265] Virginia und New Orleans verboten die Technologie vollständig.[266] Viele Orte sind von den Verboten aber mittlerweile wieder abgerückt.[267]

---

261 *Hill*, The New York Times v. 18.1.2020, https://perma.cc/C4H9-NC6H.

262 Siehe zum Einsatz nach dem Sturm auf das Kapitol auch *Rückert*, Verfassungsblog v. 22.1.2021, https://perma.cc/B567-XXZN.

263 *Fossi/Prazan*, NBC MIAMI v. 17.8.2020, https://perma.cc/H7HM-Y8N2.

264 Zuletzt wurde über die irrtümliche Festnahme von Porcha Woodruff berichtet, *Kasulis Cho*, The Washington Post v. 7.8.2023, https://perma.cc/YMS7-8RL9. Siehe auch *Johnson*, Wired v. 7.3.2022, https://perma.cc/A37S-XVBY (zu den Festnahmen von Robert Williams, Michael Oliver und Nijeer Parks); *Johnson*, Wired v. 28.2.2023, https://perma.cc/2B2X-27RH (zur Festnahme von Alonzo Sawyer); *Hill/Mac*, The New York Times v. 31.3.2023, https://perma.cc/98M2-VMHT (zur Festnahme von Randal Reid). Zu den Fällen ausführlich Kapitel III. B. I. 1.

265 Bill S.1385 191st Leg. Mass. 2019 – An Act establishing a Moratorium on Face Recognition and Other Remote Biometic Surveillance Systems, https://malegislature.gov/Bills/191/SD671.

266 *Rabinowicz*, Harvard Journal of Law and Technology JOLT Digest, 4.5.2023, https://perma.cc/CU57-RQ9S.

267 *Rabinowicz*, Harvard Journal of Law and Technology JOLT Digest, 4.5.2023, https://perma.cc/CU57-RQ9S.

b) China

Die Verwendung von Gesichtserkennung in China wird regelmäßig als Schreckensszenario mobilisiert. Tatsächlich zeigt sich hier deutlich, welche Gefahren ein weitgehender und missbräuchlicher Einsatz der Technologie mit sich bringt. China verfügt über einen gewaltigen Überwachungsapparat; mindestens 500 Millionen Überwachungskameras sind an öffentlichen Plätzen, an Eingängen von Büros, Parkhäusern und Schulen, in Zügen und Bussen installiert.[268] Gesichtserkennung macht es nun möglich, aus diesen Datenfluten eine einzelne Person herauszugreifen und herauszufinden, wo sie sich wann aufgehalten und mit wem sie Kontakt hatte. Wie gut das Überwachungssystem funktioniert, demonstrierten die Behörden nicht zuletzt, als sie – zu Testzwecken – einen BBC-Reporter als zur Fahndung ausgeschrieben markierten und ihn dann in der Millionenstadt Guiyang innerhalb von 7 Minuten aufspürten.[269] Während *Clearview AI* in den USA gerade erst dabei ist, seine Technologie in Augmented-Reality-Brillen zu integrieren, wurde aus China bereits 2018 berichtet, dass Polizisten Sonnenbrillen mit Gesichtserkennung verwendeten, um einen Heroin-Schmuggler zu fassen und Reisende auf gefälschte Ausweise zu überprüfen.[270] Wenig überraschend hat China regelmäßig Erfolge vorzuweisen. Bei einem großen Bier-Festival in der 9-Millionen-Einwohner-Stadt Qingdao etwa wurden über 20 Verdächtige mittels Gesichtserkennung identifiziert, in Wuhu unter 3,5 Millionen Menschen ein auf der Flucht befindlicher Mordverdächtiger erkannt, der gerade bei einem Straßenverkäufer Essen kaufte.[271] Chinesische Behörden verwenden Gesichtserkennung aber auch dazu, die ethnische Minderheit der Uiguren digital zu beobachten und Informationen über ihr Kommen und Gehen zu sammeln.[272] Ihre Systeme sind auch in der Lage, Menschen nach Ethnie (Race) zu sortieren und die Polizei zu alarmieren, sobald Uiguren gesichtet werden.[273]

268 *Qian/Xiao/Mozur/Cardia*, The New York Times v. 21.6.2022, https://perma.cc/5MU8-T2PG.
269 *Russell*, TechCrunch v. 14.12.2017, https://perma.cc/VM6Q-4YAJ.
270 *Mozur*, The New York Times v. 8.7.2018, https://perma.cc/BC7A-GUN5.
271 *Mozur*, The New York Times v. 8.7.2018, https://perma.cc/BC7A-GUN5.
272 *Mozur*, The New York Times v. 14.4.2019, https://perma.cc/85V6-WAML.
273 *Bhuiyan*, Los Angeles Times v. 9.2.2021, https://perma.cc/W6SB-AD6S.

c) Russland

Russland baut ebenfalls seit Jahren sein Überwachungssystem auf regionaler und nationaler Ebene aus;[274] allein in Moskau wurden zwischen 2017 und 2022 mehr als 220.000 mit (Echtzeit-)Gesichtserkennung ausgestattete Kameras installiert.[275] Eine spezifische Rechtsgrundlage für den Einsatz von Gesichtserkennung existiert nicht;[276] die Rechte der Bürger werden nur durch die allgemeinen Normen der russischen Verfassung geschützt. Die Polizeibehörden setzen auf Gesichtserkennung, um Verdächtige zu identifizieren, aber auch um Demonstranten und Regierungskritiker wegen (angeblicher) Straftaten oder Ordnungswidrigkeiten aufzuspüren.[277] Als etwa im April 2021 Tausende Menschen in ganz Russland gegen die Inhaftierung des Oppositionspolitikers Alexey Navalny demonstrierten, nahm die Polizei umgehend zahlreiche Demonstranten gewaltsam fest. Nur in Moskau blieben die Massenfestnahmen aus. Dort wurden Dutzende Demonstranten Tage und Wochen später zu Hause oder am Arbeitsplatz festgenommen, nachdem die Polizei sie per Gesichtserkennung identifiziert hatte.[278] Insgesamt wurden auf diese Weise bereits mindestens Hunderte Demonstranten nach Anti-Kreml-Protesten identifiziert und verhaftet.[279]

Näheres darüber, wie solche Festnahmen ablaufen können, wurde anlässlich eines EGMR-Urteils[280] gegen Russland im Jahr 2023 bekannt. Der Beschwerdeführer 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.").[281] Von der Protestaktion wurden Fotos

274 Vgl. auch *Kuteynikov/Izhaev/Lebedev/Zenin*, Lex Russica 2022, 121, 127.
275 EGMR, Urt. v. 4.7.2023, 11519/20, Rn. 5.
276 *Kuteynikov/Izhaev/Lebedev/Zenin*, Lex Russica 2022, 121, 127.
277 So die russische Nichtregierungsorganisation OVD-Info, 17.1.2022, https://perma.cc/A57N-KBET.
278 *Solopov*, Meduza v. 27.4.2021, https://perma.cc/KD8C-BCGJ.
279 *Masri*, Reuters v. 28.3.2023, https://perma.cc/L7QD-B5UA.
280 EGMR, Urt. v. 4.7.2023, 11519/20. Russland ist 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 Abs. 2 EMRK.
281 Hierzu die russische Nichtregierungsorganisation OVD-Info, 4.7.2023, https://perma.cc/LTU2-X85U; in der Entscheidung des EGMR findet sich die Formulierung

und ein Video in den sozialen Medien hochgeladen; diese fand die Polizei. Mit nachträglicher Gesichtserkennung identifizierte sie den Demonstranten (Identitätsermittlung). Wenige Tage später wurde er in der U-Bahn festgenommen, offenbar lokalisiert durch Echtzeit-Gesichtserkennung.[282] Daraufhin wurde er zu einer Geldstrafe von etwa 283 Euro verurteilt, weil er seinen Protest nicht angemeldet hatte.

2. Zentrale Probleme

Der Einsatz von Gesichtserkennung bringt demnach vor allem drei Risiken mit sich: Fehlidentifizierungen und Ermittlungen gegen (gänzlich unbeteiligte) Unschuldige, Einschränkung der Privatheit des Einzelnen und dadurch potenziell Auswirkungen auf die Gesellschaft. Diese werden häufig erst sichtbar, wenn der Blick nicht auf eine einzelne Maßnahme fällt, sondern Gesichtserkennung darüber als System verstanden wird.[283]

„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.

282 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 erklärbar war, wie die Polizei den Demonstranten so schnell nach seinem Protest identifizieren konnte, EGMR, Urt. v. 4.7.2023, 11519/20 Rn. 72. Da die russische Polizei den Einsatz von Gesichtserkennung nicht dokumentieren und Betroffene auch nicht darüber informieren muss, sei es im Übrigen für die Bürger kaum möglich, den Einsatz zu beweisen.

283 Vgl. einen ähnlichen Gedanken bei *Poscher*, in: Vöneky/Kellmeyer/Müller/Burgard, The Cambridge Handbook of Responsible Artificial Intelligence, 2022, 281, 288 („[T]he alternative approach implies a more systemic perspective on data collection and data processing measures. It allows us to step back from the idea that each and every instance of personal data processing constitutes an infringement of a fundamental right. If data protection is understood as protection against abstract dangers, then we do not have to look at the individual instances of data processing. Instead, we can concentrate on the data processing system and its context in order to evaluate the abstract danger it poses."). Vgl. auch *Renan*, Stanford Law Review 2016, 1039, 1042 ff.

a) Fehlidentifizierung und Ermittlungsmaßnahmen gegen Unbeteiligte

Dass sich Ermittlungen immer auch gegen Unschuldige richten können, ist an sich nicht ungewöhnlich. Wie *Singelnstein* treffend formuliert, gehören „zulässige Maßnahmen gegen Unschuldige zum Alltag der Strafverfolgungsbehörden […], namentlich stets dann, wenn sich erst ex post die Unschuld eines Verdächtigen herausstellt".[284] Wie bereits angesprochen, wohnen der automatisierten Gesichtserkennung aber eine spezifische Gefahr und eine erhöhte Wahrscheinlichkeit inne, dass Unbeteiligte beschuldigt werden und dass der Fehler wegen großer optischer Ähnlichkeit nicht immer erkannt wird.[285] Zudem können aufgrund des Einsatzes der Gesichtserkennung gänzlich Unbeteiligte, die keinerlei Bezug zu Tat oder wirklichem Täter haben, in das Ermittlungsumfeld der Polizei geraten. Denn es wird allein an das Aussehen angeknüpft.

b) Privatheit der Betroffenen

Mit Blick auf die Betroffenen einer Gesichtserkennungsmaßnahme besteht die Gefahr, dass die Behörden die Daten zu einem Bewegungsmuster oder gar einem Persönlichkeitsprofil verknüpfen könnten.[286] Durch die Erkennung können eine Reihe von Informationen über einen Menschen gewonnen werden, einschließlich seiner beruflichen Tätigkeit, Freizeitaktivitäten und religiösen Überzeugung. Auch können Hinweise auf seine sexuelle Orientierung oder politische Ausrichtung gewonnen werden, etwa wenn er bei der Teilnahme an bestimmten Versammlungen identifiziert wird.

284 *Singelnstein*, Strafbare Strafverfolgung, 2019, 206.

285 Siehe hierzu auch die Fälle in Kapitel III. B. I. 1.

286 Siehe nur *Ferguson*, Minnesota Law Review 2021, 1105, 1117 („The resulting scans could locate individuals at any point they are identified by a camera, creating a virtual retrospective map of movements and activities over time."); *Garvie/Bedoya/Frankle*, The Perpetual Line-Up: Unregulated Police Face Recognition in America, Center on Privacy & Technology, Georgetown Law, 2016, https://perma.cc/BSF9-9A9C („If cities like Chicago equip their full camera networks with face recognition, they will be able to track someone's movements retroactively or in real-time, in secret."); *Hurtz*, Süddeutsche Zeitung v. 22.1.2020, https://perma.cc/8SWN-5AWK.

c) Auswirkungen auf die gesamte Gesellschaft

Darüber hinaus stellt sich aber eine weitere Frage, auch für diejenigen, die selbst gar nicht (zu Recht oder zu Unrecht) von Gesichtserkennung betroffen sind: Was bedeutet es für eine Gesellschaft, in der jeder darum weiß, dass er oder sie mit Leichtigkeit identifiziert werden *könnte*?

Die Metapher des Panoptikums wurde im Zusammenhang mit Überwachungsmaßnahmen schon zur Genüge verwendet. Die Frage, die sie mit Blick auf den Einsatz von Gesichtserkennung aufwirft, ist aber richtig. Führt die Sorge vor einer Überwachung dazu, dass die Menschen ihr Verhalten ändern und Abstand nehmen von – möglicherweise sogar grundrechtlich besonders geschützten – Aktivitäten wie einer Versammlungsteilnahme? Benthams Panoptikum ist eine Gefängnisarchitektur, die es ermöglicht, mit nur einem Wächter alle Gefängnisinsassen im Blick zu behalten.[287] Von einem Wachturm in der Mitte kann er in die ringsum angeordneten Zellen aller Gefangenen blicken, diese können jedoch nicht erkennen, ob sich in dem dunklen Turm gerade ein Wächter befindet. Das Entscheidende daher: Die Insassen wissen nie, ob sie gerade überwacht werden. Dadurch, so die Theorie, passen die Beobachteten ihr Verhalten aus Furcht vor Sanktionen selbst an – und das mit einem geringen Personalaufwand von Seiten des Gefängnisses. Ob ein solcher „Panoptikum-Effekt" tatsächlich besteht, ist eine andere Frage. Zumindest in autoritären Staaten ist durchaus naheliegend, dass Bürgerinnen und Bürger an Demonstrationen nicht teilnehmen, weil sie Angst vor Repressionen haben – und Gesichtserkennung ist das Ermittlungswerkzeug, um sie schnell und effektiv aufzuspüren.

3. Relevanz für Deutschland

Warum sollten diese Beispiele missbräuchlichen oder nachlässigen Umgangs mit Gesichtserkennung für eine Regulierung von Gesichtserkennung in Deutschland relevant sein? Weder wenden deutsche Strafverfolgungsbehörden autoritäre Methoden an, noch gibt es Berichte darüber, dass wegen Gesichtserkennung vermehrt gegen Unschuldige ermittelt wird. Dem ist zu entgegen:

287 *Bentham*, in: Welzbacher, Panoptikum oder Das Kontrollhaus, 2013, 7, 13 ff.

Erstens wird nicht systematisch ausgewertet, wie die weiteren Ermittlungen nach Gesichtserkennungstreffern in Deutschland verlaufen.[288] Ob und wie häufig Unschuldige aufgrund des Einsatzes von Gesichtserkennung ins Visier der Strafverfolgungsbehörden geraten, ist daher nicht bekannt. Zudem weiß ein zu Unrecht Verdächtigter womöglich gar nicht, dass wegen eines Gesichtserkennungstreffers der Verdacht auf ihn gefallen war, denn hierauf wird er nicht ausdrücklich hingewiesen; eine Benachrichtigungspflicht besteht nicht.[289] Im Rahmen einer Akteneinsicht kann er zwar den Bericht über die Gesichtserkennungsrecherche einsehen, sofern dieser in die Akten aufgenommen wird. Unverteidigte Beschuldigte werden jedoch trotz ihres Rechts darauf[290] nicht immer Einsicht in ihre Akten beantragen.[291]

Zweitens mag es zwar zutreffend sein, dass ein missbräuchlicher Umgang mit Gesichtserkennung in absehbarer Zeit in Deutschland nicht droht. Auch kann man daher in Frage stellen, ob in Deutschland tatsächlich wegen der Verwendung von Gesichtserkennung in der Strafverfolgung Einschüchterungseffekte bestehen oder in Zukunft drohen.[292] Das Bundesverfassungsgericht zieht diese Argumentationsfigur aber jedenfalls heran[293] und begründet mit ihr ebenfalls eine erhöhte Eingriffsintensität mit Blick auf die informationelle Selbstbestimmung.[294] Da das Gericht auch bei der automatisierten Kfz-Kennzeichenkontrolle mit Einschüchterungseffekten

288 Dazu bereits Kapitel I. F. I. 5.

289 Zu der in der Praxis herangezogenen Rechtsgrundlage des § 98c StPO noch ausführlich Kapitel II. C. I.

290 § 147 Abs. 4 StPO.

291 Da Gesichtserkennung besonders häufig auch bei weniger schweren Delikten herangezogen wird (Kapitel I. F. II. 1.), ist nicht unplausibel, dass viele Betroffene nicht verteidigt waren und selbst keine Akteneinsicht beantragt haben. Daher konnten sie gar nicht erfahren, dass durch eine Gesichtserkennungsrecherche (und die anschließende Identifizierung durch einen Menschen) der Verdacht auf sie fiel.

292 Zur Kritik am Konzept der Einschüchterungseffekte wegen mangelnder Empirie allgemein vgl. nur *Staben*, Der Abschreckungseffekt auf die Grundrechtsausübung, 2016, 121 ff., (speziell auch zur fehlenden Empirie für Deutschland); *Nettesheim*, VVDStRL 2011, 7, 28; *Sklansky*, California Law Review 2014, 1069, 1094 ff.; *De Mot/Faure*, Tort Law Review 2014, 120, 121.

293 Siehe nur BVerfGE 65, 1 (42); 113, 29 (46); 120, 378 (430).

294 Siehe nur BVerfGE 120, 378 (402). Andere argumentieren, dass Einschüchterungseffekte bereits zur Eröffnung des Schutzbereichs (oder zu einem Eingriff) führen, unabhängig davon, ob tatsächlich personenbezogene Daten erhoben werden, siehe nur mwN *Albrecht/Seidl*, in: Möstl/Weiner, BeckOK Polizei- und Ordnungsrecht Niedersachsen, 29. Ed., Stand: 1.11.2023, NPOG § 32 Rn. 6.

argumentiert hat,[295] ist davon auszugehen, dass es auf solche erst recht bei der automatisierten Gesichtserkennung zurückgreifen wird.[296] Auch ist nach der verfassungsgerichtlichen Rechtsprechung für das Eingriffsgewicht bereits entscheidend, welche *Möglichkeiten* des Missbrauchs eine Maßnahme birgt,[297] nicht ob sie tatsächlich missbräuchlich eingesetzt wird. Hierauf wird in Kapitel II. ausführlich eingegangen. Interessant sind in diesem Zusammenhang auch die Ausführungen des Bundesverfassungsgerichts in seiner Entscheidung zur Wiederaufnahme zuungunsten des Freigesprochenen, wonach „die verfassungsrechtlichen Anforderungen an den Gesetzgeber nicht deshalb ab[nehmen], weil eine gefestigte demokratische und rechtsstaatliche Entwicklung in der Bundesrepublik Deutschland dazu geführt hätte, dass eine Abkehr oder Aufweichung der verfassungsrechtlichen Grundsätze nicht mehr zu befürchten sind".[298] Übertragen auf Gesichtserkennung würde dies bedeuten, dass auch Gefahren in den Blick zu nehmen sind, die derzeit und in naher Zukunft noch nicht bestehen.

Drittens sind die erwähnten Gefahren und Beispiele aus anderen Staaten häufig Gegenstand medialer Berichterstattung über automatisierte Gesichtserkennung (siehe hierzu ausführlich Kapitel III.). Sie beeinflussen daher die öffentliche Wahrnehmung des Einsatzes dieser Strafverfolgungstechnologie. Eine weitgehende Überwachung in Deutschland mag nicht real sein, aber die Sorge davor kann es durchaus sein. Gerade angesichts der Tatsache, dass, wie oben erwähnt, ein großer Teil der Bevölkerung auf Künstlicher Intelligenz basierenden neuen Technologien mit Bedenken gegenübersteht, erscheint es sinnvoll, proaktiv mögliche Probleme zu identifizieren und durch eine gesetzliche Regelung zu adressieren.

295 BVerfGE 120, 378 (402); siehe auch BVerfGE 150, 244 (268): „Eine solche Maßnahme ist nicht erst hinsichtlich ihrer Folgen, sondern als solche freiheitsbeeinträchtigend. Zur Freiheitlichkeit des Gemeinwesens gehört es, dass sich die Bürgerinnen und Bürger grundsätzlich fortbewegen können, ohne dabei beliebig staatlich registriert zu werden, hinsichtlich ihrer Rechtschaffenheit Rechenschaft ablegen zu müssen und dem Gefühl eines ständigen Überwachtwerdens ausgesetzt zu sein […] Jederzeit an jeder Stelle unbemerkt registriert und darauf überprüft werden zu können, ob man auf irgendeiner Fahndungsliste steht oder sonst in einem Datenbestand erfasst ist, wäre damit unvereinbar."

296 Das gilt jedenfalls für das Einsatzszenario der Echtzeit-Fahndung.

297 Kapitel II. A. I. 2. b) ee).

298 BVerfG, NJW 2023, 3698, 3708.

H. Fazit zu Kapitel I. Grundlagen

In Deutschland setzen BKA, Bundespolizei, Landeskriminalämter und Landespolizeibehörden automatisierte Gesichtserkennung bereits regelmäßig ein, um unbekannte Verdächtige zu identifizieren. Die Technologie erfüllt dabei eine Filter- und Sortierfunktion, menschliche Experten überprüfen die Vorschläge. Auch bei schlechter Bildqualität kann Gesichtserkennung zumindest einen ermittlungsunterstützenden Hinweis geben, gegen wen nun weiter ermittelt werden soll. Bei einer Regulierung der Technologie sollten die zentralen Risiken im Blick behalten werden: Fehlidentifizierungen und Ermittlungen gegen Unschuldige, Beeinträchtigung der Privatheit der Betroffenen und mögliche Auswirkungen auf die Gesellschaft. Dadurch könnten auch die Legitimität und das Vertrauen in die Strafverfolgungsbehörden gestärkt werden.

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.

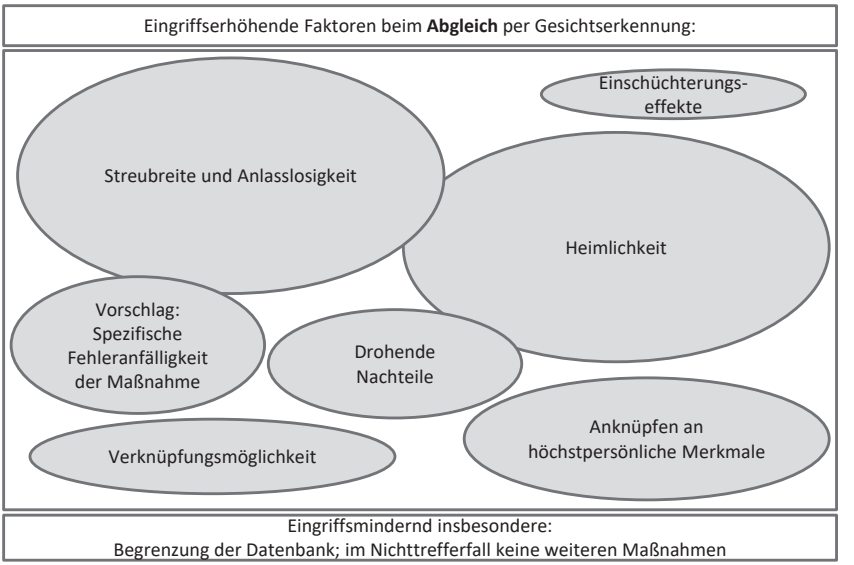

Abbildung 4: Eingriffsgewicht bestimmende Faktoren beim Abgleich mit Gesichtserkennung

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 f.); 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).

Kapitel III. Folgen und mediale Darstellung des Einsatzes automatisierter Gesichtserkennung – kriminologische Betrachtung

„Most things are never meant."
– Philip Larkin[858]

Jede neue Erfindung, jede neue Technologie soll ein Problem lösen, bringt aber auch Folgen mit sich, die nicht beabsichtigt waren. Welche Folgen der zunehmende Einsatz automatisierter Gesichtserkennung in der Strafverfolgung hat und noch haben wird, ist bislang noch unzureichend untersucht worden. In diesem Kapitel sollen zunächst die möglichen Auswirkungen auf zwei Ebenen näher betrachtet werden: Folgen für die Strafverfolgung und Folgen für Unbeteiligte. Selbstverständlich kann hier nicht der Anspruch erhoben werden, diese Fragen umfassend beantworten zu können. Es soll jedoch aufgezeigt werden, mit welchen Fragen und Problemen sich die Strafrechtswissenschaft und die Kriminologie in Zukunft werden befassen müssen. Dabei werden nicht dystopische Zukunftsszenarien, sondern konkrete Risiken betrachtet. Zunächst wird untersucht, wie sich der Einsatz automatisierter Gesichtserkennung auf die Selektivität der Strafverfolgung auswirken könnte, also darauf, welche Straftaten verfolgt und am Ende tatsächlich abgeurteilt werden und welche nicht (A.). Dann wird herausgearbeitet, wie und warum es im Zusammenhang mit Gesichtserkennung zu vermehrten Ermittlungsmaßnahmen gegen Unbeteiligte kommt; hierfür werden die Fälle der Festnahmen Unschuldiger in den USA näher ausgewertet (B.).

Zudem wird untersucht, welches Bild die Medien von dem Einsatz automatisierter Gesichtserkennung in der Strafverfolgung zeichnen. Neue Technologien, insbesondere wenn sie auf KI basieren und durch die Polizei eingesetzt werden, können eine Verunsicherung in der Gesellschaft hervorrufen und das Vertrauen in staatliches, insbesondere polizeiliches Handeln beeinträchtigen. Da die wenigsten Menschen auf Fachliteratur zu dem Thema zurückgreifen, liegt es nahe, dass die Medien einen Einfluss auf die Wahrnehmung der Technologie haben könnten. Um näher nachzuvoll-

858 *Larkin*, Collected Poems, 1988, 190.

ziehen, wie Gesichtserkennung in den Medien dargestellt wird und welche Bedenken im Vordergrund stehen, wird eine qualitative Inhaltsanalyse von Medienbeiträgen durchgeführt (C).

A. Folgen für den strafrechtlichen Selektionsprozess

„Stellen Sie sich einmal vor, daß jeder der ein Unrecht begeht, entdeckt und entsprechend bestraft wird."
– William Makepeace Thackeray[859]

Strafverfolgung ist selektiv. Nur ein Bruchteil aller Verhaltensweisen, die einen Straftatbestand erfüllen, werden tatsächlich gerichtlich abgeurteilt.[860] Dieser Selektionsprozess hängt von unterschiedlichen Faktoren ab; das Recht („first code") ist jedenfalls nicht allein ausschlaggebend, entscheidender ist die Rechtsanwendung („second code").[861] Daher genügt ein Blick auf die Rechtsnormen (Welches Verhalten ist strafbar? Wann darf die Polizei einschreiten? Welche Ermittlungsmethoden sind zulässig?) nicht. In den Blick zu nehmen sind auch die ungeschriebenen Normen, die in der Praxis faktisch entscheiden, welches Verhalten im strafrechtlichen Selektionsprozess ausgefiltert wird und welches verfolgt und geahndet wird. Die Anzeigebereitschaft der Bevölkerung für bestimmte Delikte, die Kontrolltätigkeit der Polizei, die Art und Schwere des Delikts, gesellschaftliche Machtstrukturen, die Ressourcenverteilung innerhalb der Strafverfolgungsbehörden und Kosten-Nutzen-Erwägungen sind nur einige dieser ungeschriebenen Kriterien. Welchen Einfluss neue Technologien auf diese Selektionsmechanismen haben, wird in Deutschland bislang noch kaum untersucht.[862] Im Folgenden soll auf dem Fundament bisheriger grundlegender kriminologi-

859 Zitiert nach *Popitz*, in: Pohlmann/Eßbach, Popitz, Soziale Normen, 1968, 158, 159.

860 Ausführlich etwa *Eisenberg/Kölbel*, Kriminologie, 2024, § 28 Rn. 41 ff.; § 31 Rn. 1 ff.; *Meier*, Kriminologie, 2021, § 9 Rn. 32 ff.; *Singelnstein/Kunz*, Kriminologie, 2021, § 19 Rn. 2 ff., 19 ff.; siehe auch *Neubacher*, Kriminologie, 2023, Kap. 3 Rn. 2 ff; *Dölling/Hermann/Laue*, Kriminologie, 2022, § 28 Rn. 15; *Singelnstein*, ZfR 2014, 321, 326 f.; speziell zur Selektivität der Strafverfolgung im Kontext neuer Kontrolltechnologien *Wehrheim*, in: Schmidt-Semisch/Hess, Die Sinnprovinz der Kriminalität. Zur Dynamik eines sozialen Feldes, 2014, 137.

861 Zu dieser Unterscheidung *MacNaughton-Smith*, Journal of Research in Crime and Delinquency 1968, 97; siehe auch *MacNaughton-Smith*, in: Lüderssen/Sack Seminar: Abweichendes Verhalten II, 1975, 197 ff., 210.

862 Vgl. aber *Wehrheim*, in: Schmidt-Semisch/Hess, Die Sinnprovinz der Kriminalität, 2014, 137, 150 f. Zu Überlegungen für die USA etwa *Burrell/Fourcade*, Annual Re-

scher Erkenntnisse überlegt werden, an welchen Stellen des Kriminalisierungsprozesses automatisierte Gesichtserkennung wirken und so die Selektivität der Strafverfolgung noch weiter verstärken oder verschieben kann. Diese Überlegungen können als Basis für zukünftige empirisch-kriminologische Forschung in diesem Bereich dienen.

I. Bekanntwerden von strafbarem Verhalten

Nur Taten, die zur Kenntnis der Strafverfolgungsbehörden (typischerweise der Polizei) gelangen, können strafrechtlich verfolgt werden. In den meisten Fällen ist dies auf eine Anzeige von Privaten zurückzuführen, meist von Geschädigten, teilweise auch von Zeugen.[863] Seltener sind es polizeiliche Kontrollen oder andere Ermittlungstätigkeiten, die zu einem Tatverdacht führen. Entscheidend dafür, welche strafbaren Verhaltensweisen verfolgt werden, ist daher zumeist die Frage, welche Taten überhaupt wahrgenommen, als strafbar bewertet und angezeigt werden.

1. Verstärkte Anzeigebereitschaft durch Aufzeichnung von Taten und Verdächtigen

Die Entscheidung, eine Strafanzeige zu erstatten, wird von vielen unterschiedlichen Faktoren beeinflusst.[864] Neben der wahrgenommenen Schwere des Delikts sind die angenommenen Erfolgsaussichten ein wesentliches Kriterium.[865] Der vermehrte Einsatz von Gesichtserkennung in der Straf-

view of Sociology 2021, 213. Zum Einfluss des Predictive Policing auf die Polizeiarbeit *Krasman/Egbert*, Predictive Policing, 2019, 55 ff.

863 *Singelnstein/Kunz*, Kriminologie, 2021, § 19 Rn. 19 mwN; siehe auch *Eisenberg/Kölbel*, Kriminologie, 2024, § 24 Rn. 11 und *Dölling/Hermann/Laue*, Kriminologie, 2022, § 28 Rn. 15.

864 Siehe nur *Birkel/Church/Erdmann/Hager/Leitgöb-Guzy*, Sicherheit und Kriminalität in Deutschland, 2020, 82 ff. und *Birkel/Church/Hummelsheim-Doss/Leitgöb-Guzy/Oberwittler*, Der Deutsche Viktimisierungssurvey 2017, 2019, 42 ff. zu Gründen für oder gegen eine Anzeige; *BMI/BMJ*, Zweiter Periodischer Sicherheitsbericht, 2006, 19 zu Gründen für die Nichtanzeige. Siehe auch den Überblick bei *Eisenberg/Kölbel*, Kriminologie, 2024, § 24 Rn. 13 ff.; *Neubacher*, Kriminologie, 2023, Kap. 3 Rn. 11 ff.; *Meier*, Kriminologie, 2021, § 9 Rn. 34 ff.; *Singelnstein/Kunz*, Kriminologie, 2021, § 19 Rn. 20 ff.

865 *Birkel/Church/Erdmann/Hager/Leitgöb-Guzy*, Sicherheit und Kriminalität in Deutschland, 2020, 87, 90 ff.; *Birkel/Church/Hummelsheim-Doss/Leitgöb-Gu-*

verfolgung und vor allem das *Bekanntwerden* des vermehrten Einsatzes von Gesichtserkennung innerhalb der Gesellschaft könnten dazu führen, dass in der Bevölkerung für viele Delikte höhere Erfolgsaussichten angenommen werden. Wo in der Vergangenheit keine oder kaum Ansatzpunkte bestanden, um die Identität eines unbekannten Täters zu ermitteln – etwa bei einem körperlichen Angriff durch einen Unbekannten oder einem von Menschen unbemerkten Diebstahl in einem Supermarkt –, bestehen mittlerweile Ermittlungsansätze.[866] Der Initiator einer Schlägerei in einer Diskothek könnte auf Fotos auf der Webseite des Nachtclubs abgebildet sein;[867] den Dieb könnte eine Überwachungskamera aufgezeichnet haben. Allein die Bildaufnahme half in der Vergangenheit wenig, wenn Zeugen oder die Polizei den Unbekannten nicht zufällig wiedererkannten. Automatisierte Gesichtserkennung verspricht nun, die Identität in Sekundenschnelle zu ermitteln. Es kann daher die Vermutung aufgestellt werden, dass mit dem zunehmenden Bekanntwerden der Gesichtserkennung als polizeilicher Ermittlungsmethode die wahrgenommenen Erfolgsaussichten und damit auch die Anzeigebereitschaft grundsätzlich ansteigen werden.

Gesichtserkennung könnte zudem auch indirekt dazu führen, dass mehr und mehr Straftaten überhaupt erst wahrgenommen werden. In den vergangenen Jahren war bereits ein Anstieg privater Überwachungskameras zu verzeichnen: in der Bahn, in Verkaufsflächen von Geschäften, in Hauseingängen, in Autos, in Restaurants, in Cafés, am Arbeitsplatz.[868] Wer damit rechnet, dass die Polizei per Gesichtserkennung auch unbekannte Täter identifizieren könnte, hat nun womöglich einen (weiteren) Anreiz, um eine Überwachungskamera anzubringen. Dadurch könnten in Zukunft auch deutlich mehr strafbare Verhaltensweisen überhaupt erst wahrgenommen werden. Zudem werden mehr und mehr Bild- und Videoaufnahmen mit privaten Smartphones angefertigt; für das Jahr 2027 wird prognostiziert, dass rund 70 Millionen Menschen in Deutschland ein Smartphone besitzen

---

zy/Oberwittler, Der Deutsche Viktimisierungssurvey 2017, 2019, 43, 98; *BMI/BMJ*, Zweiter Periodischer Sicherheitsbericht, 2006, 19; siehe auch *Singelnstein/Kunz*, Kriminologie, 2021, § 19 Rn. 20;

866 Vgl. auch bereits Kapitel I. G. I. 3. zu Fällen, in denen durch die Möglichkeit der Gesichtserkennung Spurenansätze bestehen.

867 Zu diesem Fall Kapitel I. G. I. 3.

868 *Weichert* im Gespräch mit Ensminger, „Immer mehr Überwachung um uns herum", Deutschlandfunk v. 11.12.2014, https://perma.cc/9DJZ-VQE7; hierzu auch *Eisenberg/Kölbel*, Kriminologie, 2024, § 27 Rn. 71; *Hoffmann*, Der nichtstaatliche Einsatz biometrischer Gesichtserkennungssysteme nach der DSGVO, 2023, 30 f.

werden.[869] Werden hierbei auch Delikte oder Verdächtige aufgezeichnet, besteht mit Gesichtserkennung nun eine erhöhte Wahrscheinlichkeit, dass strafbares Verhalten geahndet werden kann. Dies kann auch einen zusätzlichen Anreiz geben, Geschehen mit dem Handy aufzuzeichnen. Das BKA rechnet bereits damit, dass „[a]ufgrund des steigenden Aufkommens digitaler Aufnahmen, z. B. in den sozialen Netzwerken und der durch Smartphones allzeitigen Möglichkeit Bilder zu fertigen, […] in den nächsten Jahren mit einem weiteren Anstieg der Zahl der GES-Recherchen zu rechnen" ist.[870]

Wichtig wird bei all dem sein, im Blick zu behalten, *welche Straftaten* überhaupt visuell aufgezeichnet werden (können), denn diese dürften in Zukunft auch noch verstärkter wahrgenommen werden. Diebstähle und Körperverletzungen (bzw. die Täter beim Betreten oder Verlassen des Tatorts) werden eher von einer Kamera aufgezeichnet werden als Bilanzfälschungen und Steuerhinterziehungen (dazu auch sogleich im nächsten Abschnitt 2. unten). Den Umstand, dass u. a. Wirtschaftsdelikte weniger sichtbar und daher schwerer zu ahnden sind,[871] wird der Einsatz automatisierter Gesichtserkennung also nicht ändern.[872] Stattdessen könnte es zu einer noch stärkeren Verschiebung der strafverfolgungsbehördlichen Ressourcen hin zu den visuell wahrnehmbaren, ohnehin bereits im Fokus der Öffentlichkeit stehenden Delikten kommen.

Insbesondere könnte automatisierte Gesichtserkennung dazu führen, dass Klein- und Bagatellkriminalität häufiger verfolgt wird, etwa Beleidigungen oder Diebstähle geringwertiger Sachen. War der Täter dem Geschädigten, einem Zeugen oder den Behörden nicht bekannt, so war eine

869 *Statista*, Anzahl der Smartphone-Nutzer* in Deutschland in den Jahren 2009 bis 2022 und Prognose bis 2027 (in Millionen), https://de.statista.com/statistik/daten/studie/198959/umfrage/anzahl-der-smartphonenutzer-in-deutschland-seit-2010/.

870 Webseite des Bundeskriminalamts, Gesichtserkennung, https://perma.cc/NZ3K-B555.

871 *Meier*, Kriminologie, 2021, § 11 Rn. 14.

872 Vgl. zu einem ähnlichen Gedanken im Bereich der Gefahrenabwehr *Rademacher/Perkowski*, JuS 2020, 713, 717 allgemein mit Blick auf KI-gestützte Technologien: „KI-gestützte Technologien funktionieren vielmehr nur hoch spezifisch in Bereichen, in denen ausreichend digitalisierte Daten vorhanden sind, um die jeweilige Software damit für den Einsatz ‚trainieren' zu können. Nur dann können die oben erwähnten Suchmuster geformt werden. Gefahren, die selten oder (noch) nicht digital erfassbar sind, drohen damit zugunsten gut erfassbarer Gefahren vom Radar der Polizei zu verschwinden."

Identifizierung in der Vergangenheit kaum möglich. Eine Veröffentlichung von Lichtbildern zur Identitäts- und Aufklärungsfahndung nach § 131b Abs. 1 StPO ist nur zulässig beim Verdacht einer Straftat von erheblicher Bedeutung (dies ist im Einzelfall zu bestimmen[873]). Bei Bagatelldelikten waren daher eine solche Identitätsaufklärung und somit eine Strafverfolgung nicht möglich. Es existierten keine konkreten Zahlen dazu, wie viele leichte und bagatellarische Delikte derzeit verfolgt werden; die Strafverfolgungsstatistik schlüsselt nicht auf, welchen Wert z. B. beim Diebstahl die entwendete Sache hatte.[874] Taten von Erst- oder Gelegenheitstätern werden typischerweise aus Opportunitätsgründen eingestellt (§ 153 StPO oder § 45 Abs. 1 JGG);[875] solche Verfahren laufen standardisiert ab und werden nur „verwaltet", zu Vernehmungen oder anderen Ermittlungen, Anklagen und Hauptverhandlungen kommt es kaum.[876] Anders verlaufen Verfahren hingegen bei wiederholt auffällig gewordenen Personen, auch wenn diese jedes Mal nur mit Bagatelldelikten in Erscheinung getreten sind. Die Ursachen für diese Mehrfachauffälligkeit können vielfältig sein; *Bernd-Dieter Meier* nennt beispielsweise prekäre Lebensverhältnisse, Interesse- und Gedankenlosigkeit, Drogenprobleme, die desintegrierenden Auswirkungen vorangegangener Sanktionen oder den Wunsch nach mehr Aufmerksamkeit.[877] Für die Justiz ändert dies jedoch regelmäßig nichts daran, dass bei wiederholter Straftatbegehung selbst im Bagatellbereich das öffentliche Interesse an der Strafverfolgung bejaht wird, sodass eine Einstellung nach § 153 StPO nicht mehr in Betracht kommt. Der Betroffene wird daher angeklagt und mit einer Geldstrafe oder Bewährungsstrafe sanktioniert.[878] Kommt es weiterhin zu Straftaten, so kann irgendwann wegen ungünstiger Legalprognose (vgl. § 56 StGB) selbst bei Bagatellkriminalität letztendlich eine Freiheitsstrafe ohne Bewährung folgen.[879] Diese Entwicklung droht sich mit dem vermehrten Einsatz automatisierter Gesichtserkennung noch

873 Siehe nur BeckOK StPO/*Niesler*, 49. Ed., Stand: 1.10.2023, StPO § 131 Rn. 6; der Begriff der Straftat von erheblicher Bedeutung entspricht dem des § 131 Abs. 3 StPO.

874 Bei generell bagatellhaften Delikten wie der Beförderungserschleichung lässt sich zumindest die Anzahl der verfolgten Taten ermitteln. Mit Blick auf die Verurteilungen differenziert die Strafverfolgungsstatistik wegen einer solchen Tat allerdings nicht danach, ob zugleich noch andere Taten verwirklicht wurden.

875 *Meier*, in: FS Rössner, 2015, 304, 304 f.

876 *Singelnstein/Kunz*, Kriminologie, 2021, § 19 Rn. 28 mwN.

877 *Meier*, in: FS Rössner, 2015, 304, 305.

878 Siehe hierzu nur *Meier*, in: FS Rössner, 2015, 304, 306 ff.

879 Kritisch etwa *Kinzig*, in: FS Schöch, 2010, 647; vgl. auch *Beulke*, in: FS Heinz, 2012, 594.

zu verschärfen. Gesichtserkennung wird nicht auf bestimmte Straftaten beschränkt. Nach einer Äußerung des Leiters der Abteilung Cybercrime beim bayerischen Landeskriminalamt gibt es „praktisch kein Delikt, wo das keine Rolle spielt", darunter auch Beleidigungen, Betrug und klassische Ladendiebstähle.[880] Dabei seien schwere Delikte „zahlenmäßig nicht so häufig vertreten".[881] Wenn eine Strafverfolgungstechnologie es der Polizei so leicht macht, unbekannte Ladendiebe zu identifizieren, könnten solche Taten in Zukunft noch häufiger verfolgt werden. Das gilt insbesondere deshalb, weil eine Identifizierung nur dann möglich ist, wenn sich der Betreffende in der Datenbank befindet, also (in den meisten Fällen) bereits Beschuldigter in einem Strafverfahren war; damit gehört er erst recht zur „Klientel" der Personen, die trotz Bagatellhaftigkeit des Delikts strafrechtlich verfolgt werden. Ob eine solche noch stärkere Verfolgung von Bagatelltaten kriminalpolitisch erwünscht ist, sollte äußerst kritisch hinterfragt werden. Jedenfalls sollte eine solche Entwicklung nicht als unbeabsichtigte Nebenfolge des Einsatzes automatisierter Gesichtserkennung unbemerkt und unreflektiert bleiben.

2. Polizeiliche Videoaufzeichnungen

Polizeiliche Kontrollen und andere Ermittlungstätigkeiten können ebenfalls einen Tatverdacht begründen. Auch hier kann die Vermutung aufgestellt werden, dass die Polizei in Kenntnis der Möglichkeiten der Gesichtserkennung einen immer größeren Anreiz haben wird, staatliche Videoüberwachung an öffentlichen Plätzen auszubauen[882] und häufiger Bodycams[883] und Drohnen[884] zu verwenden.[885] Freilich müssen diese Maßnahmen weiterhin die rechtlichen Voraussetzungen erfüllen, eine Videoüberwachung öffentlicher Plätze beispielsweise ist also weiterhin nur zulässig, wenn

880 *Jordan*, Bayerischer Rundfunk v. 1.6.2021, https://perma.cc/7FQS-3WQS.
881 *Jordan*, Bayerischer Rundfunk v. 1.6.2021, https://perma.cc/7FQS-3WQS.
882 Zum Anstieg staatlicher Überwachungskameras etwa *Szymanski*, Süddeutsche Zeitung v. 27. Februar 2013, https://perma.cc/2A3R-2V7T.
883 Zur nachgelagerten Verfolgung von Straftaten und Ordnungswidrigkeiten als einer der Zwecke des Einsatzes von Bodycams siehe nur *Schmidt*, Polizeiliche Videoüberwachung durch den Einsatz von Bodycams, 2018, 37, 39.
884 Zum Einsatz von Drohnen durch die Polizei etwa *Tomerius*, LKV 2020, 481.
885 Bereits die Videoaufzeichnung als solche (ohne Gesichtserkennung) dürfte die Erwartung erhöhen, dass Täter identifiziert werden können, vgl. *Eisenberg/Kölbel*, Kriminologie, 2024, § 27 Rn. 71 unter Verweis auf *Töpfer*, KrimJ 2009, 272, 278 ff.

sich die Kriminalitätsbelastung dort von der des übrigen Gemeindegebiets deutlich abhebt und Tatsachen die Annahme rechtfertigen, dass dort auch künftig mit der Begehung von Straftaten zu rechnen ist (so § 44 Abs. 3 BWPolG, vgl. zu den Vorgaben in anderen Bundesländern etwa § 15a Abs. 1 PolG NRW, Art. 33 BayPAG, § 14 Abs. 3 und 4 HSOG, § 32 Abs. 3 NPOG). Es steht jedoch zu vermuten, dass ein erhöhter Anreiz besteht, einen Ort als einen solchen sog. Kriminalitätsbrennpunkt einzustufen, wenn die Polizei davon ausgeht, dass die Delikte dann tatsächlich auch (sogar vergleichsweise einfach) aufgeklärt werden können – dies ermöglicht automatisierte Gesichtserkennung. Daher liegt es nahe, dass die Technologie zu mehr staatlicher Videoüberwachung führt, wodurch mehr Geschehnisse aufgezeichnet und daher auch mehr Straftaten bekannt werden.

Mit Blick auf die durch staatliche Videokameras aufgezeichneten Delikte ist wie bei den privaten Aufzeichnungen festzustellen, dass eine Verschiebung in Richtung der öffentlich visuell wahrnehmbaren Verhaltensweisen naheliegt.[886] Staatliche Videoüberwachung im öffentlichen Raum soll vor allem Straßenkriminalität erfassen.[887] Darunter fallen schwere Delikte wie Raubüberfälle (§ 249 StGB) sowie gefährliche und schwere Körperverletzung (§§ 224, 226 StGB) auf Straßen, Wegen oder Plätzen, aber auch weniger gravierende Delikte wie einfache Diebstähle und unbefugte Ingebrauchnahmen von Kraftwagen, Mopeds, Krafträdern und Fahrrädern (§§ 242, 248b StGB), einfacher Diebstahl von oder aus Automaten (§ 242 StGB) und Sachbeschädigungen (§ 303 StGB) auf Straßen, Wegen oder Plätzen.[888] Wenn der Einsatz automatisierter Gesichtserkennung tatsächlich zu einem Anstieg an staatlicher Überwachung und damit Aufzeichnung öffentlicher Plätze führt, dann würden solche Delikte – auch bagatellhafte – in Zukunft noch stärker wahrnehmbar und durch Gesichtserkennung dann auch nachverfolgbar.

Damit stellt sich auch die Frage, gegen welche Menschen sich Strafverfolgung dann vermehrt richten würde. An öffentlichen Plätzen und in Bahnhofsgegenden, die häufig videoüberwacht sein werden, dürften sich Woh-

886 Vgl. zur Videoüberwachung *Eisenberg/Kölbel*, Kriminologie, 2024, § 27 Rn. 72, auch zum Effekt der Verlagerung an andere Orte.

887 Zu dieser gesetzgeberischen Intention siehe nur LT-Dr. BW 12/5706, 7, 9, 11. Der VGH Mannheim nennt als typische Straßenkriminalität etwa Raub, Körperverletzung, Betäubungsmitteldelikte, Sachbeschädigung, Sexualdelikte, Diebstahl, insbesondere Taschendiebstahl, VGH Mannheim, NVwZ 2004, 498, 504.

888 So die Polizeiliche Kriminalstatistik, Rubrik: Straßenkriminalität.

nungslose und Menschen mit Migrationsgeschichte häufiger aufhalten.[889] Diese Personen werden dann nicht nur öfter kontrolliert,[890] ihre Handlungen werden auch vermehrt aufgezeichnet und etwaige Straftaten wahrgenommen und nachvollziehbar. Körperverletzungen, Betäubungsmitteldelikte und Diebstähle im öffentlichen Raum werden daher in Zukunft – im Vergleich zu denselben Taten im eigenen Zuhause oder im nicht überwachten Büro – noch wesentlich häufiger aufgedeckt und verfolgt werden, als dies ohnehin bereits der Fall ist. Das kann insbesondere dann problematisch sein, wenn durch eine solche Verschiebung der Strafverfolgung (und ihrer Ressourcen) andere Delikte wie etwa Wirtschaftsstraftaten, die womöglich noch mehr Schäden anrichten, weniger intensiv verfolgt würden. Jedenfalls sollte auch hier eine mögliche Verlagerung der Ressourcen nicht unbemerkt und unreflektiert bleiben.

II. Weitere Ermittlungen

Im Rahmen weiterer Ermittlungen durch die Polizei kann die automatisierte Gesichtserkennung ebenfalls an entscheidenden Stellschrauben auf den Selektionsprozess in der strafrechtlichen Sozialkontrolle einwirken. Das liegt zum einen daran, dass ein höherer Ermittlungsaufwand betrieben wird, wenn der antizipierte Ermittlungsaufwand überschaubar bleibt.[891] Ergeben sich also zu Beginn der Ermittlungen bereits erfolgversprechende Anhaltspunkte für die Aufklärung, werden weitere Ermittlungen mit größerer Intensität betrieben. Delikte werden insbesondere mit einer höheren Wahrscheinlichkeit aufgeklärt, wenn sich die Ermittlungen nicht gegen unbekannt, sondern gegen eine bestimmte Person richten.[892] Eine Untersuchung von *Dölling* ergab beispielsweise, dass bei Einbruchdiebstahl, Raub, Vergewaltigung und Betrug die Aufklärungswahrscheinlichkeit bereits im

889 Vgl. zu dieser Überlegung mit Blick auf Menschen mit Migrationsgeschichte *Bliesener*, Ausländer- und Zuwandererkriminalität, 2018, 14; vgl. auch *Wehrheim*, in: Schmidt-Semisch/Hess, Die Sinnprovinz der Kriminalität, 2014, 137, 138 mit der Feststellung, dass es keine empirischen Hinweise darauf gebe, dass in innerstädtischen Fußgängerzonen als unerwünscht betrachtete „Punks oder Obdachlose" allein deshalb einen Ort verließen, weil sie von einer Kamera beobachtet würden.

890 *Niemz/Singelnstein*, in: Hunold/Singelnstein Rassismus in der Polizei, 2022, 337, 345; *Müller*, Kriminalität, Kriminalisierung und Wohnungslosigkeit, 2006, 120 mwN.

891 *Meier*, Kriminologie, 2021, § 9 Rn. 47 mwN.

892 *Singelnstein/Kunz*, Kriminologie, 2021, § 19 Rn. 27.

„ersten Angriff" deutlich erhöht ist, wenn der Geschädigte oder ein Tatzeuge den Namen des Tatverdächtigen nennen konnten.[893] Wenn der Name nicht genannt werden konnte, sank die Aufklärungswahrscheinlichkeit deutlich.[894] Ist ein Foto des Verdächtigen vorhanden, kann die Polizei mit automatisierter Gesichtserkennung mittlerweile in Sekundenschnelle den Namen einer Person ermitteln.

1. Auffindbarkeit in Datenbanken

Das gilt allerdings nur, wenn der Verdächtige auch in der durchsuchten Datenbank zu finden ist. Mit dem Gesichtserkennungssystem GES des BKA kann INPOL-Z durchsucht werden; wenn Polizeibehörden lokal ein Gesichtserkennungssystem verwenden, können sie ihre lokalen Datenbestände durchsuchen.[895] Hier liegt eine weitere, ganz wesentliche Weichenstellung im strafrechtlichen Selektionsprozess: Nur wer in der Datenbank gespeichert ist, kann identifiziert werden. Ein und dieselbe Körperverletzung, ein und derselbe Diebstahl hat daher eine deutlich höhere Aufklärungswahrscheinlichkeit, wenn der Täter in der Vergangenheit erkennungsdienstlich behandelt wurde.

Eine problematische polizeiliche Kontrolltätigkeit (etwa signifikant häufigere Kontrollen bei als ausländisch oder als sozioökonomisch schwach wahrgenommenen Personen), die es zugleich wahrscheinlicher macht, dass der Betroffene erkennungsdienstlich behandelt wird, wirkt sich daher an dieser Stelle erneut aus. Vermehrte Kontrollen bei bestimmten Personengruppen führen dann nicht nur dazu, dass diese häufiger bestraft werden, weil bei diesen Kontrollen Straftaten festgestellt werden. Sie werden auch häufiger bestraft, weil *in Zukunft* strafbares Verhalten ihnen erneut per Gesichtserkennung zugeordnet werden kann.

Dabei darf zudem nicht vergessen werden, dass in den mit dem GES durchsuchbaren Datenbanken nicht nur Personen gespeichert sind, die wegen des Verdachts einer Straftat erkennungsdienstlich behandelt wurden, sondern insbesondere auch verdachtsunabhängig alle Asylbewerber. Wenn diese Delikte begehen und ein Bild von ihnen vorhanden ist, steigt die

893 *Dölling*, Polizeiliche Ermittlungstätigkeit und Legalitätsprinzip, Erster Halbband, 1987, 258 ff.

894 *Dölling*, Polizeiliche Ermittlungstätigkeit und Legalitätsprinzip, Erster Halbband, 1987, 258.

895 Zu INPOL-Z als durchsuchbarer Datenbank für das GES siehe Kapitel I. F. I. 1.

Aufklärungswahrscheinlichkeit daher signifikant an. Und auch wenn das Verfahren eingestellt wird: Das (erneute) Ermittlungsverfahren wird notiert und kann dazu führen, dass in künftigen Fällen nicht mehr mit einer Einstellung des Verfahrens zu rechnen ist. Automatisierte Gesichtserkennung wird daher dazu führen, dass die Strafverfolgung in Fällen, in denen ein Lichtbild eines unbekannten Verdächtigen vorhanden ist, sich mehr und mehr verschiebt hin zu Personen, die bereits in der Vergangenheit in Kontakt mit der Polizei kamen oder aus anderen Gründen erkennungsdienstlich behandelt wurden.

Eine Beschränkung der durchsuchbaren Datenbank ist daher ambivalent zu betrachten: Einerseits verringert eine Begrenzung die Streubreite der Gesichtserkennungssuche und die Anzahl der Personen, die fälschlicherweise als Täter identifiziert werden könnten. Andererseits wirkt sie aber auch massiv auf den strafrechtlichen Selektionsprozess ein und bewirkt eine Verschiebung der strafverfolgungsbehördlichen Ressourcen hin zu den Personen, die in der Datenbank erfasst sind.

2. Anreiz zur Erfassung in Datenbanken

Darüber hinaus besteht durch die Möglichkeiten automatisierter Gesichtserkennung ein erheblicher Anreiz, mehr und mehr Personen in den durchsuchbaren Datenbanken zu erfassen. Nur wer dort gespeichert ist, kann gefunden werden; je mehr Personen gespeichert sind, desto „besser" also. Dies könnte dazu führen, dass zum Beispiel mit Blick auf erkennungsdienstliche Behandlungen nach § 81 Abs. 1 Alt. 2 StPO schneller eine Wiederholungsgefahr angenommen wird,[896] um die Person im System erfassen zu können. Zukünftige empirisch-kriminologische Forschung könnte daher beispielsweise der Frage nachgehen, ob die Anzahl erkennungsdienstlicher Behandlungen signifikant ansteigt, wenn in einer Polizeibehörde die Bekanntheit und Verbreitung automatisierter Gesichtserkennung zunimmt. Sollte dies zutreffen, dann könnten all diese nun erfassten Personen ebenfalls in späteren Strafverfahren erkannt werden. Damit würde automatisierte Gesichtserkennung erneut eine Ausweitung der Strafverfolgung bei den Delikten bewirken, bei denen (typischerweise) Lichtbilder von Tat oder Täter vorhanden sind.

896 Zu § 81b Alt. 2 StPO siehe bereits Kapitel II. A. I. 2. b) bb).

III. Fazit

Automatisierte Gesichtserkennung birgt nicht nur das (nicht unkritisch zu sehende) Potenzial, dass in Zukunft mehr und mehr Delikte verfolgt und aufgeklärt werden können. Sie droht auch auf die ohnehin bestehende Selektivität der Strafverfolgung verstärkt einzuwirken. Die Technologie bewirkt eine Verschiebung der Strafverfolgungsressourcen hin zu Straftaten, die (insbesondere in der Öffentlichkeit) visuell wahrnehmbar und erfassbar sind. Zudem droht eine intensivere Verfolgung von Bagatellkriminalität, insbesondere bei Wiederholungstätern.

Beschränkungen der durchsuchbaren Datenbanken sind daher ambivalent zu sehen. Einerseits verringert eine Beschränkung die Streubreite der Gesichtserkennungsmaßnahme und die Anzahl der Personen, die potenziell als der Verdächtige fehlidentifiziert werden könnten. Andererseits bewirkt die Beschränkung eine immer stärkere Verschiebung der Verfolgung hin zu Personen, die bereits in der Vergangenheit mit der Polizei interagiert haben oder die aus anderen Gründen in den durchsuchbaren Datenbanken gespeichert sind (z. B. Asylsuchende).

Diese Überlegungen sollen nicht in Abrede stellen, dass es sich auch bei Bagatelldelikten und visuell wahrnehmbaren Taten um Straftaten handelt. Um Straftaten handelt es sich aber auch bei den gegen Strafgesetze verstoßenden Verhaltensweisen, die schwer visuell wahrzunehmen und auf Video aufzuzeichnen sind (Stichwort: Wirtschaftsdelikte) und die durch Personen begangen werden, die nicht in per Gesichtserkennung durchsuchbaren Lichtbilddatenbanken gespeichert sind. Es ist vor allem die mit Gesichtserkennung potenziell einhergehende verstärkte *Verschiebung* der Strafverfolgung hin zu (auch) Bagatelldelikten und Menschen, die in Gesichtserkennungsdatenbanken gespeichert sind, die es zu reflektieren gilt.

Solche Entwicklungen sollten nicht unbemerkt voranschreiten, sondern kriminologisch näher untersucht und kritisch hinterfragt werden. Die in diesem Abschnitt erarbeiteten Gedanken können als Hypothesen den Ausgangspunkt für künftige empirisch-kriminologische Forschung bilden.

B. Folgen für Unbeteiligte

„Error is part of policing."
– Andrew Guthrie Ferguson[897]

Kein Ermittlungswerkzeug, keine Ermittlungsmaßnahme ist fehlerfrei. Der automatisierten Gesichtserkennung wohnt jedoch eine spezifische Fehleranfälligkeit inne: Sie kann gänzlich Unbeteiligte erfassen, die nicht einmal in der Nähe des Tatorts waren, und Fehler sind schwerer zu erkennen, denn der Betroffene sieht schließlich aus wie der Verdächtige. Ob es im Zusammenhang mit dem Einsatz automatisierter Gesichtserkennung in Deutschland vermehrt zu Ermittlungen gegen Unbeteiligte kam, ist nicht bekannt. Die Verfahren, in denen die Polizei den Verdächtigen per Gesichtserkennung identifiziert hat, werden nicht systematisch ausgewertet und daraufhin überprüft, in wie vielen und in welchen Fällen Personen beschuldigt wurden, die sich am Ende als unschuldig herausstellten. Dass es hierzu auch, anders als in den USA, keine Medienberichte über die Erfahrungen Betroffener gibt, bedeutet nicht zwingend, dass solche Fälle nicht vorkommen. Vielmehr kann die fehlende Berichterstattung auch daran liegen, dass der Einsatz automatisierter Gesichtserkennung den Beschuldigten gar nicht bekannt war. Eine Pflicht zur Benachrichtigung über die Verwendung von Gesichtserkennung existiert im deutschen[898] Strafprozessrecht nicht,[899] und selbst wenn der Einsatz in den Akten vermerkt sein sollte, ist nicht davon auszugehen, dass die meisten unverteidigten Beschuldigten selbst Akteneinsicht beantragen.

Um besser nachvollziehen zu können, wie es im Zusammenhang mit Gesichtserkennung zu Ermittlungsmaßnahmen gegen Unbeteiligte kommt und welche Ursachen dem zugrunde liegen, werden im Folgenden die Fälle der Festnahme Unschuldiger in den USA nach falschen Gesichtserkennungstreffern näher beleuchtet.[900] Dadurch sollen auch Erkenntnisse

897 *Ferguson*, Minnesota Law Review 2021, 1105, 1173.

898 Auch in den USA sind gegenwärtig weder auf nationaler noch – soweit ersichtlich – auf bundesstaatlicher oder lokaler Ebene Benachrichtigungspflichten beim Einsatz von Gesichtserkennung geregelt; die Betroffenen erfahren hiervon nur, wenn dies offengelegt oder in den Akten vermerkt und vom Verteidiger entdeckt wird, siehe *Jackson*, The Champion 2019, 14, 16 und Kapitel III. B. I. 3. a).

899 Hierzu bereits Kapitel II. C. I. 1. b) mit Blick auf den in der Praxis herangezogenen § 98c StPO.

900 Einige der Erkenntnisse in diesem Abschnitt beruhen auf Überlegungen, die ich in meinem LL.M. Paper „Blame The Human, Not (Just) The Algorithm – Regulating

darüber gewonnen werden, wie solche Folgen für Unbeteiligte auch in Deutschland verhindert werden können.

I. Festnahme Unbeteiligter in den USA nach falschem Gesichtserkennungstreffer

Aus den USA sind bereits sechs Fälle bekannt gewordenen, in denen Unschuldige nach einem falschen Gesichtserkennungstreffer als Verdächtige identifiziert wurden. Diese sollen im Folgenden näher betrachtet (1.) und kurz rechtlich eingeordnet werden (2.). Es liegt außerdem nahe, dass es weitere Fälle gibt, die lediglich nicht bekannt geworden sind; auch hierauf wird eingegangen (3.).

1. Bekannt gewordene Fälle

a) Michael Oliver

Im Juli 2019 wurde Michael Oliver auf dem Weg zur Arbeit bei einer Verkehrskontrolle in Ferndale, Michigan, festgenommen.[901] Die Polizei informierte ihn, dass ein Haftbefehl gegen ihn vorliege. Der Vorwurf: schwerer Diebstahl (Felony larceny).[902] Er solle einem Lehrer, der eine Schlägerei vor einer Schule aufzeichnete, das Smartphone entrissen und es auf den Boden geworfen haben.[903] Der Lehrer hatte das Video mit der Polizei geteilt, die daraus einen Screenshot des Täters anfertigte.[904] Anhand dieses Screenshots identifizierte eine Gesichtserkennungssoftware den bereits vorbestraften Oliver als Ermittlungshinweis (Investigative lead). Bei einer anschließenden Wahllichtbildvorlage (Photo lineup) mit sechs

---

Facial Recognition Technology to Prevent Wrongful Arrests" an der Harvard Law School im akademischen Jahr 2022/23 entwickelt habe. Das Paper ist noch unveröffentlicht; es wurde bei der Writing Competition 2023 der Georgetown Law Technology Review und des Institute for Technology Law & Policy an der Georgetown Law School eingereicht und mit einem Writing Prize ausgezeichnet.

901 *Johnson*, Wired v. 7.3.2022, https://perma.cc/A37S-XVBY.

902 *Anderson*, Detroit Free Press v. 10.7.2020, https://perma.cc/XD3Y-976R.

903 *Johnson*, Wired v. 7.3.2022, https://perma.cc/A37S-XVBY.

904 *Johnson*, Wired v. 7.3.2022, https://perma.cc/A37S-XVBY.

Bildern identifizierte der Lehrer Oliver als den Täter.[905] Er wurde daraufhin drei Tage lang in Polizeigewahrsam gehalten und verlor infolge der Festnahme seinen Job als Lackierer von Autoteilen. Erst Monate später bei der Anhörung vor Beginn des Prozesses (Pre-trial hearing) sah Oliver erstmals die Beweise gegen ihn: den Screenshot des unbekannten Verdächtigen. Sein Anwalt wies den Richter darauf hin, dass Oliver eine andere Statur und, anders als der auf dem Screenshot abgebildete Täter, Tätowierungen auf den Armen und über der linken Augenbraue habe.[906] Daraufhin wurde die Anklage fallen gelassen.

b) Nijeer Parks

Nijeer Parks betrat im Februar 2019 das Woodbridge Police Department, New Jersey. Seine Großmutter hatte ihm mitgeteilt, dass die Polizei aus Woodbridge in der 30 Meilen (ca. 50 km) entfernten gemeinsamen Wohnung in Paterson, New Jersey, nach ihm gesucht habe.[907] Parks begab sich zur Polizeistation, um die Situation zu klären. Stattdessen wurde er festgenommen und verbrachte zehn Tage in Haft.[908] Die Vorwürfe wogen schwer: Er habe Snacks und Süßigkeiten aus einem Geschenkartikelladen eines Hotels in Woodbridge gestohlen, einen Polizeibeamten beinahe mit dem Auto angefahren, eine schwere Körperverletzung begangen, sei unrechtmäßig im Besitz von Waffen gewesen, habe einen gefälschten Ausweis benutzt, Marihuana besessen, den Tatort verlassen und sich der Festnahme widersetzt.[909] Damit drohten ihm Jahre im Gefängnis, zumal Parks bereits wegen Drogendelikten vorbestraft war. Der Täter hatte einen gefälschten Ausweis verwendet und am Tatort zurückgelassen; das Bild wurde per Gesichtserkennung gescannt und daraufhin Parks als Verdächtiger ins Auge gefasst.[910] Der Gesichtserkennungstreffer war, soweit bekannt, hierfür der einzige Anhaltspunkt.

Etwa ein halbes Jahr später, noch bevor eine Verhandlung anberaumt war, kaufte Parks ein neues Smartphone und ging bei dieser Gelegenheit

905 *Anderson*, Detroit Free Press v. 10.7.2020, https://perma.cc/XD3Y-976R.
906 *Stokes*, CBS News v. 19.11.2020, https://perma.cc/AM59-9P7P.
907 *Johnson*, Wired v. 7.3.2022, https://perma.cc/A37S-XVBY.
908 *General/Sarlin*, CNN Business v. 29.4.2021, https://perma.cc/9PT6-HKD8.
909 *General/Sarlin*, CNN Business v. 29.4.2021, https://perma.cc/9PT6-HKD8.
910 *General/Sarlin*, CNN Business v. 29.4.2021, https://perma.cc/9PT6-HKD8.

alte Fotos durch. Dabei fand er zufällig den Screenshot einer Quittung für eine Western-Union-Überweisung an seine Verlobte. Diese Überweisung hatte er etwa zur gleichen Zeit getätigt, wie der ihm vorgeworfene Diebstahl stattfand. Da die Western Union in Paterson, New Jersey, 30 Meilen (ca. 50 km) von dem Hotelladen entfernt war, konnte Parks seine Unschuld beweisen.[911] Bis dahin hatte es fast ein Jahr gedauert.

c) Robert Williams

Der erste bekannt gewordene und wohl am meisten berichtete Fall der Festnahme eines Unbeteiligten nach einer Gesichtserkennungsrecherche betraf Robert Julian-Borchak Williams.[912] An einem Donnerstagnachmittag im Januar 2020 verhaftete die Polizei ihn in seinem Vorgarten vor den Augen seiner Frau und seiner beiden kleinen Töchter und legte ihm Handschellen an.[913] Er wurde in eine Haftanstalt gebracht und dort über Nacht festgehalten. Einer der Polizisten, die ihn am nächsten Tag befragten, zeigte Williams ein Standbild aus einem Überwachungsvideo, das in einem Geschäft in Detroit aufgenommen worden war. Es waren fünf Uhren im Wert von 3.800 Dollar gestohlen worden. Auf dem Bild war vor einer Uhrenauslage ein schwergewichtiger Mann zu sehen, der schwarz gekleidet war und eine rote St. Louis Cardinals-Mütze trug. „Sind Sie das?", fragte der Ermittler. Er zeigte Williams ein weiteres Bild, eine Nahaufnahme. Das Foto war unscharf, es zeigte aber offensichtlich nicht Williams. Dieser hielt das Bild neben sein Gesicht. „Nein, das bin ich nicht", sagte er. „Denken Sie, dass alle schwarzen Männer gleich aussehen?" Nachdem die Polizisten die Nahaufnahme des Verdächtigen neben dem Gesicht von Williams gesehen hatten, erkannten sie den Unterschied ebenfalls. Einer von ihnen sagte zu dem anderen: „Ich glaube, der Computer hat sich geirrt." („I guess the computer got it wrong.").[914]

911 *Johnson*, Wired v. 7.3.2022, https://perma.cc/A37S-XVBY.
912 *Hill*, The New York Times v. 3.8.2020, https://perma.cc/QUF9-RQQF.
913 *Hill*, The New York Times v. 3.8.2020, https://perma.cc/QUF9-RQQF.
914 *Hill*, The New York Times v. 3.8.2020, https://perma.cc/QUF9-RQQF.

d) Alonzo Sawyer

Im März 2022 geriet ein etwa 30-jähriger schwarzer Mann in Streit mit einer Busfahrerin.[915] Sie forderte ihn auf, eine Maske zu tragen, und zog ihr Handy heraus, um die Polizei zu rufen, als er sich weigerte. Der Mann nahm ihr das Handy weg und rannte nach draußen, die Busfahrerin hinterher; dort schlug er ihr ins Gesicht.[916] Das Geschehen wurde von einer Überwachungskamera aufgezeichnet.[917] Polizisten der Maryland Transit Administration Police extrahierten aus diesem Video mehrere Standbilder des Täters und leiteten sie zur Kenntnisnahme (Be on the Lookout bulletin) an die Strafverfolgungsbehörden weiter.[918] Daraufhin beschloss eine Analystin bei der Staatsanwaltschaft, eine Gesichtserkennungsrecherche durchzuführen.[919] Das Suchbild generierte eine Liste mit potenziellen Treffern; unter diesen identifizierte die Analystin den 54-jährigen Alonzo Sawyer als bestes Match. Kurz darauf nahm eine Einheit des Baltimore Police Department ihn fest.[920] Seine Frau nahm sich eine Woche von der Arbeit frei, um ihn aus der Haft zu holen. Sie zeigte auf der Polizeistation aktuelle Bilder ihres Mannes vor und wies darauf hin, dass dieser größer und viel älter sei als der Verdächtige im Video und zudem einen Bart und eine sichtbare Zahnlücke habe.[921] Sawyer wurde nach neun Tagen aus der Haft entlassen. Etwa zur selben Zeit identifizierte die Busfahrerin einen anderen Mann als den Verdächtigen im Video, der 17 cm kleiner und über 20 Jahre jünger als Alonzo Sawyer war.[922]

915 *Press*, The New Yorker v. 13.11.2023, https://www.newyorker.com/magazine/2023/11/20/does-a-i-lead-police-to-ignore-contradictory-evidence.
916 *Johnson*, Wired v. 28.2.2023, https://perma.cc/2B2X-27RH.
917 *Press*, The New Yorker v. 13.11.2023, https://www.newyorker.com/magazine/2023/11/20/does-a-i-lead-police-to-ignore-contradictory-evidence.
918 *Press*, The New Yorker v. 13.11.2023, https://www.newyorker.com/magazine/2023/11/20/does-a-i-lead-police-to-ignore-contradictory-evidence.
919 *Press*, The New Yorker v. 13.11.2023, https://www.newyorker.com/magazine/2023/11/20/does-a-i-lead-police-to-ignore-contradictory-evidence.
920 *Johnson*, Wired v. 28.2.2023, https://perma.cc/2B2X-27RH.
921 *Johnson*, Wired v. 28.2.2023, https://perma.cc/2B2X-27RH.
922 *Johnson*, Wired v. 28.2.2023, https://perma.cc/2B2X-27RH.

e) Randal Reid

Randal Reid war auf dem Weg zu einem verspäteten Thanksgiving-Essen mit seiner Mutter, als die Polizei ihn in der Nähe seines Zuhauses in Atlanta, Georgia, anhielt. Er wurde beschuldigt, Designerhandtaschen im Wert von 10.000 Dollar mit einer gestohlenen Kreditkarte in einem Geschäft in einem Vorort von New Orleans, Louisiana, gekauft zu haben – drei Bundesstaaten und sieben Stunden von seiner Heimatstadt entfernt.[923] Auch aus diesem Überwachungskameravideo wurde ein Standbild extrahiert und dieses in ein Gesichtserkennungsprogramm eingespeist. Reid wurde als der Verdächtigen identifiziert und fast eine Woche lang festgehalten.[924] Als die Polizei feststellte, dass er nicht der Täter sein konnte, musste er umgehend wieder freigelassen werden: Reid hatte ein Muttermal im Gesicht und war etwa 20 Kilogramm leichter als der Verdächtige.[925]

f) Porcha Woodruff

Im Jahr 2023 wurde der erste Fall einer Frau bekannt, die im Zusammenhang mit Gesichtserkennung unschuldig festgenommen wurde. Porcha Woodruff war im achten Monat schwanger, als vor ihrer Haustür sechs Polizisten auftauchten und ihr mitteilten, dass sie festgenommen sei.[926] Ihr wurde vorgeworfen, einen bewaffneten Fahrzeugraub (Carjacking) an einer Tankstelle begangen zu haben. Sie verbrachte elf Stunden in Haft, bevor sie gegen eine Kaution von 100.000 Dollar freigelassen wurde.[927] Nach eigenen Angaben begab sie sich daraufhin in ein Krankenhaus, wo bei ihr und ihrem ungeborenen Kind eine niedrige Herzfrequenz und eine Dehydrierung diagnostiziert und behandelt werden mussten.[928] Erst später fand sie heraus, dass wegen eines Gesichtserkennungstreffers der Verdacht auf sie gefallen war. Ein aus dem Überwachungsvideo der Tankstelle extrahiertes Bild der Verdächtigen war per Gesichtserkennung ausgewertet worden, ein acht Jahre altes Foto von Woodruff erschien als möglicher Treffer.[929] Das

923 *Quach*, The Register v. 3.1.2023, https://perma.cc/LB93-YK96.
924 *Barker*, Louisiana News v. 5.1.2023, https://perma.cc/Y576-XUZA.
925 *Quach*, The Register v. 3.1.2023, https://perma.cc/LB93-YK96.
926 *Kasulis Cho*, The Washington Post v. 7.8.2023, https://perma.cc/YMS7-8RL.
927 *Bhuiyan*, The Guardian v. 15.8.2023, https://perma.cc/7A38-C5EZ.
928 *Kasulis Cho*, The Washington Post v. 7.8.2023, https://perma.cc/YMS7-8RL.
929 *Kasulis Cho*, The Washington Post v. 7.8.2023, https://perma.cc/YMS7-8RL.

Foto war angefertigt worden, als sie wegen Fahrens ohne Fahrerlaubnis festgenommen worden war. Dieses acht Jahre alte Foto inkludierte die Polizei in eine Wahllichtbildvorlage, im Rahmen derer der Geschädigte Woodruff als Beteiligte des Fahrzeugraubs identifizierte.[930] Die Ermittlungsakte enthielt keinen Hinweis, dass die Verdächtige schwanger gewesen sei.[931] Einen Monat später wurde die Anklage gegen Woodruff wegen mangelnder Beweise fallen gelassen.

2. Einordnung: Waren diese Festnahmen falsch (wrongful) oder rechtswidrig?

Bevor die Gründe für mögliche weitere (unbekannte) Fälle untersucht werden, soll kurz eingeordnet werden, wie diese nach US-amerikanischem Recht zu bewerten sind. Ob und in welchen Fällen die Festnahme Unschuldiger gegen die Verfassung, insbesondere den Vierten Verfassungszusatz (Fourth Amendment), verstößt, ist umstritten.[932] Dieser Zusatzartikel zur Verfassung schützt unter anderem vor willkürlichen Festnahmen (Unreasonable seizures). Für eine Festnahme sind insbesondere hinreichende Verdachtsmomente (Probable cause) erforderlich. Mit Blick auf den Einsatz von Gesichtserkennung argumentieren einige überzeugend, dass eine Festnahme, die allein auf einer Gesichtserkennung beruht, keinen hinreichenden Verdacht begründet und daher gegen den Vierten Verfassungszusatz verstößt.[933] Höchstrichterliche Rechtsprechung existiert jedoch bislang nicht.[934]

In den Medien wurden die Festnahmen häufig als „Wrongful arrests" bezeichnet,[935] allerdings hat dieser Begriff keine klar definierte rechtliche

930 *Bhuiyan*, The Guardian v. 15.8.2023, https://perma.cc/7A38-C5EZ.
931 *Bhuiyan*, The Guardian v. 15.8.2023, https://perma.cc/7A38-C5EZ.
932 Es kommt zudem ein Verstoß gegen die Gleichstellungsklausel des 14. Verfassungszusatzes (Equal Protection Clause) in Betracht; ein solcher wird im Zusammenhang mit dem Einsatz von Gesichtserkennung in der Strafverfolgung aber kaum je darzulegen sein; hierzu auch *Congressional Research Service*, Facial Recognition Technology and Law Enforcement: Select Constitutional Considerations, 2020, 23 ff.
933 *Benedict*, Washington & Lee Law Review 2022, 849, 880 ff.
934 Siehe auch *Congressional Research Service*, Facial Recognition Technology and Law Enforcement: Select Constitutional Considerations, 2020, 17 ff.
935 Siehe nur *Bhuiyan*, The Guardian v. 27.4.2023, https://perma.cc/3E62-5USC („First man wrongfully arrested because of facial recognition testifies as California weighs new bills"); *Johnson*, Wired v. 7.3.2022, https://perma.cc/A37S-XVBY („How Wrong-

Bedeutung. Er wird in der rechtswissenschaftlichen Literatur häufig im Zusammenhang mit „Wrongful convictions" (etwa: falschen Verurteilungen) verwendet; dieser Begriff umfasst sowohl Verurteilungen von faktisch unschuldigen Personen als auch Verurteilungen mit Verfahrensfehlern, welche die Rechte des Verurteilten verletzten.[936] Verurteilungen gelten also sowohl dann als „wrongful", wenn Rechtsfehler vorliegen, als auch wenn Unschuldige verurteilt werden. In ähnlicher Weise könnte der Begriff „Wrongful arrest" daher sowohl die Festnahme einer faktisch unschuldigen Person umfassen als auch eine Festnahme, die gegen das Recht verstößt. Im Zusammenhang mit Gesichtserkennung würde dies bedeuten, dass eine Festnahme „wrongful" ist, wenn entweder eine unschuldige Person aufgrund eines fehlerhaften Gesichtserkennungsergebnisses oder wenn eine Person unter Verletzung ihrer verfassungsmäßigen Rechte festgenommen wird. Dagegen könnte jedoch argumentiert werden, dass die Festnahme einer – wie sich im Nachhinein herausstellt – unschuldigen Person nicht „wrongful" ist, wenn die rechtlichen Voraussetzungen gewahrt waren. Denn während es bei einer Verurteilung gerade darauf ankommt, nur Schuldige zu verurteilen, ist zum Zeitpunkt einer Festnahme (oder Ermittlungsmaßnahme) noch nicht klar, ob der Verdächtige tatsächlich der Täter ist.

Ob die oben erwähnten Fälle der Festnahme Unschuldiger rechtswidrig oder falsch („wrongful") waren, ist daher nicht eindeutig. Dies ändert jedoch nichts daran, dass sie jedenfalls aus kriminalpolitischer Sicht problematisch und zu verhindern sind.

3. Gründe für mögliche weitere (unbekannte) Fälle

Bislang wurden sechs Fälle bekannt, in denen Unschuldige nach einem falschen Gesichtserkennungstreffer festgenommen wurden; jedes Mal waren die Betroffenen Schwarze. Wie viele andere Personen im Zusammenhang mit Gesichtserkennung zu Unrecht verhaftet oder sogar verurteilt worden

ful Arrests Based on AI Derailed 3 Men's Lives"); *Ikonomova*, Deadline Detroit v. 25.6.2020, https://perma.cc/C66N-D33W („Duggan Defends Detroit's Use Of Facial Recognition After Wrongful Arrest").

936 National Institute of Justice, https://nij.ojp.gov/topics/justice-system-reform/wrongful-convictions [https://perma.cc/HJ6U-ALCC] („A conviction may be classified as wrongful for two reasons: 1. The person convicted is factually innocent of the charges. 2. There were procedural errors that violated the convicted person's rights").

sein könnten, ist schwer abzuschätzen. Es gibt verschiedene Gründe, warum mögliche weitere Fälle nicht ans Licht kommen:

a) Verwendung von Gesichtserkennung wird nicht offengelegt

Zunächst gibt die Polizei in den USA oft nicht zu erkennen, dass Gesichtserkennung Teil der Ermittlungen war.[937] In Haftbefehlen oder eidesstattlichen Erklärungen verwendet die Polizei häufig vage Formulierungen wie „Identifizierungsversuch" („attempt to identify") oder „Ermittlungswerkzeug" („investigative means"), anstatt offen zu benennen, dass Gesichtserkennungstechnologie eingesetzt wurde.[938] Die Strafverteidigerin *Kaitlin Jackson* erklärt, wie der Einsatz von Gesichtserkennungstechnologie regelmäßig verschleiert wird:

> *„Police use FRS [facial recognition software] to zero in on a suspect. Once they have a suspect, law enforcement does additional investigation to collect other incriminating evidence (sometimes compelling and sometimes not) against the suspect. Often, but not always, the additional investigation will include putting the suspect in an identification procedure for a human witness to identify. The police and prosecution then rely on the other incriminating evidence when drafting the charging documents. By the time the defense attorney enters her notice of appearance, the use of FRS may be so deeply buried that, unless the attorney knows to look for it, she may never discover it was used at all."*[939]

937 *Jackson*, The Champion 2019, 14, 16.

938 *Valentino-DeVries*, The New York Times v. 12.1.2020, https://perma.cc/M7LL-DY24.

939 *Jackson*, The Champion 2019, 14, 16. Übersetzung: „Die Polizei verwendet Gesichtserkennungssoftware, um den Verdacht auf eine Person einzugrenzen. Sobald sie einen Verdächtigen identifiziert haben, führen die Strafverfolgungsbehörden zusätzliche Ermittlungen durch, um weitere belastende Beweise (manchmal überzeugend und manchmal nicht) gegen den Verdächtigen zu sammeln. Oft, aber nicht immer, bedeuten diese zusätzlichen Ermittlungen, dass der Verdächtige in ein Identifizierungsverfahren einbezogen wird, bei dem er von einem menschlichen Zeugen identifiziert werden kann. Die Polizei und die Staatsanwaltschaft stützen sich dann bei der Erstellung der Anklageschrift auf diese anderen belastenden Beweise. Zu dem Zeitpunkt, an dem die Verteidigerin bekannt gibt, dass sie an dem Verfahren teilnimmt (Notice of appearance), kann der Einsatz von Gesichtserkennungssoftware so tief vergraben sein, dass die Anwältin möglicherweise nie entdeckt, dass Gesichtserkennung überhaupt eingesetzt wurde, sofern sie nicht weiß, wonach sie suchen muss."

Die Verwendung automatisierter Gesichtserkennung wird also dadurch im Dunkeln gehalten, dass die Strafverfolgungsbehörden sich bei der Anklage auf andere Beweise stützen, die den Verdächtigen als Täter ausmachen. Bei den von *Jackson* erwähnten Identifizierungsverfahren dürfte es sich in den meisten Fällen um Wahllichtbildvorlagen (Photo lineups) handeln. Bei diesen werden einem Zeugen (meist sechs) Bilder vorgelegt, darunter eines des per Gesichtserkennung identifizierten Verdächtigen, und der Zeuge aufgefordert, hieraus den Täter auszuwählen. Diese Identifizierung wird dann als Beweis herangezogen, nicht der ursprüngliche Gesichtserkennungstreffer, der unerwähnt bleibt.

b) Keine Aufdeckung des Fehlers wegen Annahme eines Plea bargain

Zudem liegt nahe, dass in einer Reihe von Fällen der Gesichtserkennungsfehler nicht bekannt wurde, weil die Beschuldigten sich auf einen Plea bargain eingelassen haben und anschließend verurteilt wurden, obwohl sie unschuldig waren.[940] Bei einem Plea bargain macht die Staatsanwaltschaft dem Angeklagten ein Zugeständnis (in der Regel eine geringere Strafe oder eine Anklage wegen eines weniger schweren Delikts) im Gegenzug für ein Schuldbekenntnis; es kommt dann nicht zu einem Gerichtsverfahren (Trial).[941] Lediglich 1 bis 5 % der Strafverfahren in den USA werden durch Gerichtsverfahren entschieden.[942] Die mit großem Abstand meisten Fälle enden mit einem Plea deal, einem Schuldbekenntnis. Der US Supreme Court spricht daher mit Blick auf die Strafjustiz auch von einem „system of pleas, not a system of trials".[943] Die Praxis des Plea bargaining steht stark in der Kritik, weil sie nicht nur ganz wesentlich zu den astronomischen In-

940 *Garvie*, ACLU News & Commentary v. 24.6.2020, https://perma.cc/TP78-XWC8] („We cannot account for the untold number of other people who have taken a plea bargain even though they were innocent, or those incarcerated for crimes they did not commit because a face recognition system thought they looked like the suspect. But the numbers suggest that what happened to Mr. Williams is part of a much bigger picture.").

941 Siehe Webseite des Department of Justice, https://perma.cc/PGL5-YRBP.

942 *Crespo*, Columbia Law Review 2018, 1303, 1375 (Tabelle 1).

943 Lafler v. Cooper, 566 U.S. 156, 170 (2012) („Ninety-seven percent of federal convictions and ninety-four percent of state convictions are the result of guilty pleas.").

haftierungszahlen in den USA („mass incarceration") beiträgt,[944] sondern auch problematische Anreize schafft: Aufgrund ihres Ermessensspielraums können die Staatsanwälte den Angeklagten mit stark überhöhten Anklagen (mit Blick auf die vorgeworfenen Delikte oder die Höhe der Strafe) drohen[945] und im Gegenzug eine wesentlich niedrigere Strafe anbieten. Dies schafft einen sehr starken Anreiz für – selbst unschuldige[946] – Angeklagte, sich auf ein solches Angebot einzulassen und damit die Ungewissheit eines Gerichtsverfahrens zu vermeiden.

Es ist daher wenig überraschend, dass beispielsweise Nijeer Parks, obwohl er unschuldig war, darüber nachdachte, den vom Staatsanwalt angebotenen Plea deal anzunehmen.[947] Da er bereits wegen Drogendelikten in Haft war,[948] musste er im Falle eines Prozesses eine sehr harte Strafe befürchten.[949] Auch Alonzo Sawyer äußerte später gegenüber Reportern, dass er ein Schuldbekenntnis abgegeben hätte, wenn seine Frau sich nicht so engagiert für ihn eingesetzt hätte, da ihm vor Gericht 25 Jahre Gefängnis drohten.[950] Hätten die Männer den von der Staatsanwaltschaft angebotenen Plea deal angenommen, wäre nie ans Licht gekommen, welche Rolle ein falscher Gesichtserkennungstreffer bei ihrer Verhaftung gespielt hatte.

944 Hierzu ausführlich *Crespo*, Fordham Law Review 2022, 1999, 2005 ff.; siehe auch *Crespo*, Columbia Law Review 2018, 1303, 1312 ff.; *Fisher*, Yale Law Journal 2000, 857, 893.

945 Dabei drohen Staatsanwälte häufig auch Strafen an, die sie selbst nicht für angemessen halten, denn dies gibt ihnen mehr Verhandlungsmacht. Siehe etwa United States v. Kupa, 976 F. Supp. 2d 417, 420 (E.D.N.Y. 2013) („[T]o coerce cooperation . . . prosecutors routinely threaten ultra-harsh, enhanced mandatory sentences that no one—not even the prosecutors themselves—thinks are appropriate."); vgl. hierzu auch *Crespo*, Columbia Law Review 2018, 1303, 1339.

946 Siehe nur *Gazal-Ayal*, Cardozo Law Review 2005, 2295, 2304: „[Even] innocent defendants are willing to accept minor punishment in return for avoiding the risk of a much harsher trial result."

947 *Hill*, The New York Times v. 6.1.2021, https://perma.cc/N5SG-WSQ4.

948 *General/Sarlin*, CNN Business v. 29.4.2021, https://perma.cc/9PT6-HKD8.

949 *Johnson*, Wired v. 7.3.2022, https://perma.cc/A37S-XVBY („That's when it started hitting me, like a plea deal might not be bad even if I didn't do it […] because with a trial there's more [time], and me being a convicted felon, my time is doubled.").

950 *Press*, The New Yorker v. 13.11.2023, https://www.newyorker.com/magazine/2023/11/20/does-a-i-lead-police-to-ignore-contradictory-evidence.

c) Keine offensichtlichen Unterschiede zwischen Täter und Verdächtigtem

Zudem ist es möglich, dass weitere Fälle der Festnahme (oder sonstigen Maßnahmen) gegen Unschuldige nicht bekannt wurden, weil der Fehler den Behörden nicht aufgefallen ist. Die meisten der bekannt gewordenen und oben besprochenen Fälle haben eines gemeinsam: Es gab offensichtliche Unterschiede im Aussehen zwischen dem tatsächlichen Täter und dem unschuldig Verdächtigten. Michael Oliver hatte eine andere Statur und, anders als der Täter, Tätowierungen auf den Armen und über der linken Augenbraue. Als Robert Williams das Bild des Täters neben sein Gesicht hielt, erkannten die Polizisten selbst die Unterschiede im Aussehen. Reid hatte ein Muttermal im Gesicht und war etwa 20 Kilogramm leichter als der Täter. Alonzo Sawyer war 17 cm größer und über 20 Jahre älter als der Täter. Porcha Woodruff war, anders als die Täterin, hochschwanger. Nur Parks, der dem Täter offenbar sehr ähnlich sah, musste seine Unschuld auf anderem Wege beweisen, nämlich indem er die Quittung für eine Geldüberweisung vorlegte, die etwa zur gleichen Zeit wie der Ladendiebstahl stattfand, aber viele Kilometer vom Tatort entfernt war. Was aber passiert, wenn eine unschuldige Person dem Täter zwar sehr ähnlich sieht, aber nicht zufällig einen Überweisungsbeleg hat, der beweist, dass sie zum Tatzeitpunkt weit vom Tatort entfernt war?

Durch den Einsatz von Gesichtserkennung könnte die Zahl der fälschlichen Identifizierungen steigen.[951] Denn die Technologie ist besonders gut darin, Übereinstimmungen von Personen zu präsentieren, die dem Verdächtigen sehr ähnlich sind; aber für die Menschen, die diese Übereinstimmungen dann überprüfen sollen – Polizeibeamte oder Augenzeugen – ist es dadurch besonders schwierig, konsistent und zuverlässig zwischen echten Übereinstimmungen und Doppelgängern zu unterscheiden.[952] Daher könnte es sein, dass noch viel mehr unschuldige Menschen nach

951 *Moy*, William & Mary Bill of Rights Journal 2021, 337, 359 („When law enforcement use of face recognition yields a false lead who resembles the true perpetrator, eyewitnesses are likely to be tricked into erroneously identifying the lead in a showup or lineup because the lead looks like the perpetrator.").

952 *Moy*, William & Mary Bill of Rights Journal 2021, 337, 367: „As a result, misidentifications may simply be an unavoidable outcome of law enforcement use of face recognition technology. Worse, the extent to which this technology coupled with eyewitness identification may be driving misidentifications and wrongful convictions—a potentially tremendous harm—has not been measured, thus making it impossible to perform an informed analysis regarding how big the problem is and what should be done about it."

einem falschen Gesichtserkennungstreffer Ermittlungsmaßnahmen unterzogen (oder sogar verurteilt) wurden, als die sechs Fälle vermuten lassen.

d) Keine öffentliche Bekanntmachung des Falls

Ein Grund, warum weitere Fälle nicht bekannt wurden, kann schlicht darin liegen, dass der Fall keine Schlagzeilen machte, selbst wenn der Verdächtigte (oder sein Verteidiger) herausgefunden haben, dass Gesichtserkennung verwendet worden war. Zum einen liegt es durchaus nahe, dass Betroffene nach den monatelangen Ermittlungen und der Ungewissheit, was passieren wird, diese Episode in ihrem Leben möglichst schnell hinter sich lassen und nicht medial aufbereitet sehen wollen.[953] Zum anderen gehört eine Festnahme wohl zu den für die Betroffenen belastendsten Folgen eines unerkannt gebliebenen falschen Gesichtserkennungstreffers. Es ist wahrscheinlich, dass in deutlich mehr Fällen zwar keine Festnahme erfolgte, der wegen Gesichtserkennung zu Unrecht Verdächtigte aber zumindest Vernehmungen und andere Ermittlungsmaßnahmen unterzogen wurde – was ebenfalls belastende Wirkung haben kann.

e) Fazit

Möglicherweise sind noch deutlich mehr Menschen von falschen Gesichtserkennungstreffern und anschließenden Ermittlungsmaßnahmen betroffen, als die Medienberichte in den USA nahelegen. Der Einsatz von Gesichtserkennung wird von der Polizei meist nicht offengelegt, es ist zu vermuten, dass Fehler nicht entdeckt wurden, weil die zu Unrecht Verdächtigten einen Plea deal angenommen haben, und es ist zu befürchten, dass Augenzeugen wegen großer optischer Ähnlichkeit den (aufgrund von Gesichtserkennung ausgewählten) Verdächtigten fälschlicherweise als Täter identifizieren. Diese Risiken sind für die USA noch nicht näher empirisch untersucht worden.[954] In Deutschland gibt es nicht einmal eine Debatte darüber. Wenn-

953 So musste etwa Nijeer Parks beinahe ein Jahr in Unsicherheit warten, bis die Anklage gegen ihn fallen gelassen wurde, siehe *General/Sarlin*, CNN Business v. 29.4.2021, https://perma.cc/9PT6-HKD8 („What followed was a year-long legal nightmare for Parks, who faced years in prison and the potential of additional time due to his prior convictions.").

954 *Moy*, William & Mary Bill of Rights Journal 2021, 337, 367

gleich die Gefahren des Plea bargaining im deutschen Rechtssystem nicht bestehen; der Umstand, dass die Beschuldigten nicht ausdrücklich über den Einsatz von Gesichtserkennung informiert werden, trifft auch für Deutschland zu.[955] Ebenso besteht die Gefahr, dass Augenzeugen bei einer Wahllichtbildvorlage fälschlicherweise (ebenfalls) den zu Unrecht Verdächtigten identifizieren, weil dieser dem Täter sehr ähnlich sieht.

II. Ursachen der Festnahmen

Um zu verhindern, dass in Deutschland ähnliche Fälle wie in den USA eintreten, sollen die Ursachen im Folgenden näher untersucht werden. Nach den Festnahmen lauteten die Schlagzeilen jedes Mal ähnlich, bei Randal Reid beispielsweise „Facial Recognition Technology Jailed a Man for Days",[956] „Man wrongly jailed by facial recognition"[957] und „Innocent man arrested after facial recognition failed again"[958]. Die Verantwortung wurde dem Gesichtserkennungssystem zugeschrieben. Reids Fall zeigt aber weniger ein Versagen der Gesichtserkennung als vielmehr ein menschliches Versagen. Warum haben die Polizeibeamten nicht gezögert, als sie Reid festnahmen? Entweder haben sie das Muttermal in seinem Gesicht und den großen Gewichtsunterschied nicht bemerkt, oder sie haben beides bemerkt und ihn trotzdem verhaftet. Beides wäre keine gute Polizeiarbeit gewesen.

Im Folgenden werden die verschiedenen Arten der Fehler, die zu Ermittlungen gegen Unschuldige führen können, herausgearbeitet: Fehler der Technologie (1.), Fehler von Menschen (2.) und Fehler in der Mensch-Maschine-Interaktion (3.). Dabei soll es nicht darum gehen, ob die Fehler vorwerfbar sind oder nicht. Da diese Arbeit das Ziel hat, eine Rechtsgrundlage für Gesichtserkennung zu erarbeiten, liegt stattdessen der Fokus darauf, ob und wie solche Fehler durch rechtliche Vorgaben zu verhindern sind.

955 Es besteht keine Benachrichtigungspflicht, denn § 101 Abs. 4 StPO gilt nicht für Maßnahmen nach § 98c StPO, auf den in der Praxis Gesichtserkennungsrecherchen gestützt werden, siehe Kapitel II. C. I. 1. b).

956 *Thanawala*, AP News v. 25.9.2023, https://perma.cc/6PU3-PB8F.

957 *Quach*, The Register v. 3.1.2023, https://perma.cc/LB93-YK96.

958 *Barker*, Louisiana News v. 5.1.2023, https://perma.cc/Y576-XUZA.

1. Fehler der Technologie

Der Ausgangspunkt für Ermittlungen gegen Unbeteiligte im Zusammenhang mit Gesichtserkennung liegt in einem falschen Gesichtserkennungstreffer. Sowohl in Deutschland als auch, soweit ersichtlich, in den USA wird Gesichtserkennung zur Identifizierung Unbekannter so eingesetzt, dass eine Kandidatenliste mit potenziellen Übereinstimmungen generiert wird. Es ist daher systemimmanent, dass auch falsche Treffer angezeigt werden. Dies muss nicht *per se* problematisch sein, denn kein Ermittlungswerkzeug, keine Ermittlungsmaßnahme ist fehlerfrei. „Fehler" – im Sinne des Verdächtigens eines Unschuldigen – sind im Ermittlungsverfahren systemimmanent und nicht als solche problematisch.

Problematisch und nicht zu begründen ist es jedoch, wenn Ermittlungswerkzeuge eingesetzt werden, die so fehleranfällig sind, dass sie gänzlich ungeeignet sind, oder die nicht dem aktuellen Stand der Technik entsprechen. Das Bundesverfassungsgericht hat beispielsweise im Zusammenhang mit Sicherheitsmaßgaben bei der Vorratsdatenspeicherung festgestellt, dass die Verfassung nicht detailgenau vorgebe, welche Sicherheitsmaßgaben im Einzelnen geboten seien.[959] Es müsse jedoch ein Standard gewährleistet werden, „der unter spezifischer Berücksichtigung der Besonderheiten der durch eine vorsorgliche Telekommunikationsverkehrsdatenspeicherung geschaffenen Datenbestände ein besonders hohes Maß an Sicherheit gewährleistet. Dabei ist sicherzustellen, dass sich dieser Standard – etwa unter Rückgriff auf einfachgesetzliche Rechtsfiguren wie den Stand der Technik […] – an dem Entwicklungsstand der Fachdiskussion orientiert und neue Erkenntnisse und Einsichten fortlaufend aufnimmt".[960] Beim Einsatz von Gesichtserkennung ist daher ebenfalls zu fordern, dass nur Systeme eingesetzt werden, die dem Stand der Technik für dieses Einsatzszenario entsprechen. Fehlerfreiheit eines Systems kann hingegen nicht verlangt werden, denn dies ist technisch nicht möglich.[961]

959 BVerfGE 125, 260 (326).

960 BVerfGE 125, 260 (326). Dies dürfte für alle technischen Überwachungsmaßnahmen gelten; so ist beispielsweise auch mit Blick auf die Telekommunikationsüberwachung nach § 100a StPO geregelt, dass das eingesetzte Mittel „nach dem Stand der Technik" gegen unbefugte Nutzung zu schützen ist und dass kopierte Daten „nach dem Stand der Technik" gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen sind (§ 100a Abs. 5 S. 2 und 3 StPO).

961 Kapitel I. E. IV. 6.

2. Fehler von Menschen

Nicht das Gesichtserkennungssystem, das einen falschen Treffer geliefert hat, nahm eine offensichtlich unschuldige Person fest („Facial Recognition Technology Jailed a Man for Days"[962]), sondern ein Mensch. Bevor Ermittlungsmaßnahmen gegen Williams, Reid und die anderen Betroffenen gerichtet wurden, mussten mehrere menschliche Fehler passieren. Im Folgenden werden die verschiedenen Arten von menschlichem „Versagen" näher betrachtet.

a) Menschliche Fähigkeiten zur Überprüfung von Gesichtserkennungstreffern

Einige politische Entscheidungsträger scheinen zu glauben, dass durch die menschliche Überprüfung von Treffern falsche Identifizierungen ohne Weiteres verhindert werden können. In den Gesichtserkennungsrichtlinien (Facial recognition policies) des New York Police Department (NYPD) heißt es beispielsweise mit Blick auf mögliche falsche Treffer:

> „*Some studies have found variations in accuracy for some software products. The most important federal government study on the subject, however, noted that in ‚hybrid machine/human systems', where the software findings are routinely reviewed by human investigators, erroneous software matches can be swiftly corrected by human observers. The safeguards built into the NYPD's protocols for managing facial recognition, which provide an immediate human review of the software findings, prevent misidentification.*"[963]

962 *Thanawala*, AP News v. 25.9.2023, https://perma.cc/6PU3-PB8F.

963 NYPD, Questions and Answers Facial Recognition, https://perma.cc/S7YN-8H52. Übersetzung: „Einige Studien haben Schwankungen in der Genauigkeit einiger Softwareprodukte festgestellt. Die wichtigste Studie der Bundesregierung zu diesem Thema stellte jedoch fest, dass bei ‚hybriden maschinellen/menschlichen Systemen', bei denen die Softwareergebnisse routinemäßig von menschlichen Ermittlern überprüft werden, fehlerhafte Softwareübereinstimmungen von menschlichen Beobachtern schnell korrigiert werden können. Die Sicherheitsvorkehrungen in den Protokollen des NYPD zum Umgang mit Gesichtserkennung, die eine sofortige menschliche Überprüfung der Softwareergebnisse vorsehen, verhindern eine falsche Identifizierung."

Diese Richtlinien gehen davon aus, dass eine menschliche Kontrolle Fehlidentifizierungen vermeiden könne. Nicht berücksichtigt wurde hierbei jedoch offenbar die Forschung zu menschlichen Fähigkeiten bei der Überprüfung von Gesichtserkennungstreffern. *White*, *Dunn*, *Schmid* und *Kemp* haben etwa in einer 2015 veröffentlichten Studie die Erkennungsfähigkeiten der Nutzer eines Gesichtserkennungssystems gemessen.[964] Dabei untersuchten sie ein Einsatzszenario von Gesichtserkennung, das dem Szenario der Identifizierung unbekannter Verdächtiger sehr ähnlich ist: die Verwendung von Gesichtserkennung, um Reisepassanträge auf einen möglichen Identitätsbetrug zu überprüfen. In diesem Szenario wird ebenfalls ein 1:n-Abgleich durchgeführt, denn es wird ein Suchbild (das Bild des Antragstellers) mit einer großen Datenbank abgeglichen; als Ergebnis generiert das Gesichtserkennungssystem, wie bei der Suche nach Verdächtigen, eine Kandidatenliste.[965] Dadurch soll herausgefunden werden, ob der Antragsteller bereits einen Pass hat, der auf einen anderen Namen lautet, denn dies deutet auf einen Identitätsbetrug hin.[966] Die Studie untersuchte, in wie vielen Fällen es den menschlichen Überprüfern gelang, in einer Kandidatenliste von acht Bildern den echten Treffer zu finden, und wie oft eine falsche Person ausgewählt oder der echte Treffer fälschlicherweise nicht ausgewählt wurde. In der Hälfte der Kandidatenlisten war der echte Treffer nicht enthalten; hier hätten die Überprüfer also zu dem Ergebnis kommen sollen, dass die gesuchte Person nicht dabei ist. Dabei wurde auch die Erkennungsleistung von ungeschulten und geschulten Studienteilnehmern verglichen.

Die Ergebnisse zeigten insgesamt eine sehr schlechte Leistung bei der menschlichen Überprüfung von Gesichtserkennungstreffern. Dies galt sowohl für ungeschulte Studienteilnehmer als auch bei geschulten Passbeamten (Facial reviewers),[967] die diese Software bei ihrer täglichen Arbeit verwenden und bei der Aufgabe nicht signifikant besser abschnitten: Beide Gruppen machten in über 50 % der Fälle Identifizierungsfehler.[968] Dabei lagen die Fehler nicht nur darin, dass die Überprüfer den echten Treffer übersahen, sondern vor allem häufig darin, dass sie eine falsche Person

964 *White/Dunn/Schmid/Kemp*, PLOS One 2015, 1.
965 *White/Dunn/Schmid/Kemp*, PLOS One 2015, 1, 2.
966 *White/Dunn/Schmid/Kemp*, PLOS One 2015, 1, 2.
967 Für die Definition der facial reviewers und facial examiners verweist die Studie auf *Facial Identification Scientific Working Group*, Guidelines and recommendations for facial comparison training to competency, 2011, https://perma.cc/NL9B-KHNV.
968 *White/Dunn/Schmid/Kemp*, PLOS One 2015, 1, 5 f., 8 f.

als Treffer auswählten.[969] In rund 35 % der Fälle identifizierten sie die falsche Person, obwohl der echte Treffer in der Kandidatenliste vorhanden war.[970] Lediglich bei besonders ausgebildeten forensischen Gesichtserkennungsprüfern (Specialist facial examiners) zeigte die Studie eine höhere Leistungsfähigkeit, sie machten um rund 20 Prozentpunkte weniger Fehler als die Vergleichsgruppen der ungeschulten Teilnehmer und der geschulten Passbeamten.[971] Sie übersahen zwar ebenso häufig einen echten Treffer, wählten aber deutlich seltener den falschen Kandidaten aus der Liste aus.[972] Allerdings war auch ihre Erkennungsleistung nicht fehlerfrei.[973] Ein Zusammenhang zwischen der Erkennungsleistung einerseits und der Beschäftigungsdauer (und damit der Erfahrung in der Überprüfung von Gesichtserkennungstreffern) der geschulten Passbeamten sowie der ausgebildeten Gesichtserkennungsprüfer anderseits zeigte sich nicht.[974] Die Studienautoren kommen insgesamt zu dem Schluss, dass bei Gesichtserkennungssystemen, die eine Überprüfung der Ergebnisse durch einen Menschen vorsehen, die Erkennungsleistung des Systems als Ganzem stark durch die menschliche Leistungsfähigkeit begrenzt („constrained") ist.[975]

b) Überprüfung des Treffers am Computer

Die Ergebnisse von *White* et al. machen deutlich, dass eine menschliche Kontrolle der Treffer am Computer das Problem der Fehlidentifizierungen nicht löst. Der Umstand, dass eine menschliche Überprüfung vorgesehen ist, darf für deutsche Strafverfolgungsbehörden und den Gesetzgeber keine Begründung dafür sein, sich nicht mit diesem Risiko zu befassen.

Zudem legen die Studienergebnisse nahe, dass eine Rechtsgrundlage für den Einsatz von Gesichtserkennung in der Strafverfolgung vorsehen sollte, dass nur besonders ausgebildete Experten die Überprüfung der Treffer vornehmen dürfen. Ohne eine solche Regelung dürfte jeder beliebige Polizist, dessen Dienststelle ein eigenes Gesichtserkennungssystem angeschafft hat,

969 *White/Dunn/Schmid/Kemp*, PLOS One 2015, 1, 6 (Fig. 2 MISID).
970 *White/Dunn/Schmid/Kemp*, PLOS One 2015, 1, 6 (Fig. 2 MISID Adult).
971 *White/Dunn/Schmid/Kemp*, PLOS One 2015, 1, 8 f.
972 *White/Dunn/Schmid/Kemp*, PLOS One 2015, 1, 9.
973 *White/Dunn/Schmid/Kemp*, PLOS One 2015, 1, 8 (Fig. 3 MISID).
974 *White/Dunn/Schmid/Kemp*, PLOS One 2015, 1, 9.
975 *White/Dunn/Schmid/Kemp*, PLOS One 2015, 1, 10.

mit der Kontrolle der Ergebnisse betraut werden. Dies birgt jedoch ein zu hohes Fehlerrisiko.

c) Überprüfung des Treffers vor Ort

In den Fällen von Michael Oliver, Randal Reid, Robert Williams, Alonzo Sawyer und Porcha Woodruff wurde noch ein weiterer Fehler deutlich. Wenn schon die Gesichtserkennungsprüfer am Computer die Fehlidentifizierung nicht erkannten, so hätte dies jedenfalls den Polizisten auffallen müssen, als sie die Betroffenen vor Ort aufsuchten. Soweit ersichtlich, verglichen sie aber vor den Festnahmen nicht das Bild des Täters mit der nun verdächtigten Person. Bei Randal Reid bemerkten die Polizisten offenbar nicht, dass er ein Muttermal im Gesicht hatte und rund 20 Kilogramm leichter war als der Täter. Robert Williams musste erst das Bild des Täters neben seines halten, damit die Polizisten selbst erkannten, dass es sich um verschiedene Personen handelte. Hätten die Polizisten dies selbst überprüft, bevor sie Williams festnahmen, wären ihm 30 Stunden in Haft erspart geblieben.

d) Verwendung problematischen Inputs („Garbage in, Garbage out")

Fehler können auch auf problematische Input-Daten bei der Verwendung automatisierter Gesichtserkennung zurückzuführen sein.[976] Besonders deutlich macht dies ein Fall des NYPD, von dem das Georgetown Law Center on Privacy & Technology berichtet.[977] Im April 2017 nahm eine Überwachungskamera einen Verdächtigen auf, der in einem Geschäft in New York City Bier gestohlen haben soll. Das Videomaterial war jedoch so verpixelt, dass das Gesichtserkennungssystem des NYPD keine Treffer lieferte. Die Beamten der Facial Identification Section (FIS), die für die Durchführung von Gesichtserkennungssuchen für das NYPD zuständig sind, hätten zu dem Schluss kommen müssen, dass der Verdächtige nicht

976 Siehe auch United States v. Esquivel-Rios, 725 F.3d 1231, 1234 (10th Cir. 2013) (Gorsuch, J.) („Garbage in, garbage out. Everyone knows that much about computers: you give them bad data, they give you bad results.").

977 *Garvie*, Garbage in, garbage out, Center on Privacy & Technology, Georgetown Law, 2019, https://perma.cc/J64B-MPQ8.

durch Gesichtserkennung identifiziert werden kann. Sie hatten jedoch eine andere Idee. Nachdem ein Beamter festgestellt hatte, dass der Verdächtige auf dem verpixelten Bild dem Schauspieler Woody Harrelson ähnelte, verwendete er ein hochauflösendes Bild des Schauspielers anstelle des Verdächtigen für die Suche.[978] Aus der daraus resultierenden Trefferliste identifizierten die Beamten eine Person, von der sie glaubten, dass sie mit dem Verdächtigen übereinstimmt.[979] Sie schickten diese „Übereinstimmung" zurück an die ermittelnden Beamten, die schließlich eine Person wegen kleinen Diebstahls verhafteten.[980]

In einem anderen Fall versuchte die FIS die Identität des Verdächtigen eines Überfalls mit einem Bild eines Spielers der Basketballmannschaft New York Knicks zu ermitteln.[981] Es ist nicht klar, ob in diesen Fällen am Ende die richtige Person verhaftet wurde. Jedoch erhöht die Verwendung des Fotos eines anderen (wenn auch eines Doppelgängers) anstelle des Fotos des Verdächtigen die Wahrscheinlichkeit, dass die falsche Person identifiziert wird. Erst recht gilt dies, wenn keine Lichtbilder, sondern forensische Skizzen für die Gesichtserkennungssuche verwendet werden. Dem Bericht des Georgetown Law Center on Privacy & Technology zufolge gestatten jedoch einige Polizeidienststellen die Suche nach Gesichtern anhand von forensischen Skizzen, also handgezeichneten oder computergenerierten zusammengesetzten Gesichtern auf der Grundlage von Zeugenbeschreibungen.[982]

Solche Praktiken sollten wegen der erhöhten Fehleranfälligkeit untersagt werden. Eine strafprozessuale Rechtsgrundlage sollte durch ihren Wortlaut deutlich machen, dass nur Lichtbilder des Verdächtigen abgeglichen werden dürfen. Alternativ könnte dies in den RiStBV festgelegt werden.

978 *Garvie*, Garbage in, garbage out, Center on Privacy & Technology, Georgetown Law, 2019, https://perma.cc/J64B-MPQ8.

979 *Garvie*, Garbage in, garbage out, Center on Privacy & Technology, Georgetown Law, 2019, https://perma.cc/J64B-MPQ8.

980 *Garvie*, Garbage in, garbage out, Center on Privacy & Technology, Georgetown Law, 2019, https://perma.cc/J64B-MPQ8.

981 *Garvie*, Garbage in, garbage out, Center on Privacy & Technology, Georgetown Law, 2019, https://perma.cc/J64B-MPQ8.

982 *Garvie*, Garbage in, garbage out, Center on Privacy & Technology, Georgetown Law, 2019, https://perma.cc/J64B-MPQ8. Siehe aus technischer Sicht *Klare/Li/Jain*, IEEE Transactions on Pattern Analysis and Machine Intelligence 2011, 639.

e) Problematische weitere Polizeiarbeit

Daneben kann auch fragwürdige weitere Polizeiarbeit zur Festnahme einer unschuldigen Person führen. Im Fall von Nijeer Parks beispielsweise nahmen die Polizisten ihn offenbar allein auf Basis des Gesichtserkennungstreffers fest.[983] Dieses Match schien ihnen aber bereits hinreichende Verdachtsmomente (Probable cause) für die Festnahme geliefert zu haben. Dies erscheint fragwürdig, wenn man die Fehlerquoten der Gesichtserkennung und insbesondere die noch höheren Fehlerquoten bei People of Color bedenkt.[984] Tatsächlich sind sich, soweit ersichtlich, zumindest auf dem Papier alle US-amerikanischen Strafverfolgungsbehörden (sowohl auf lokaler als auch auf Bundesebene) einig, dass ein Gesichtserkennungstreffer allein kein hinreichender Grund für eine Festnahme sein kann.[985] Das NYPD zum Beispiel erklärt in ihren Richtlinien zur Verwendung von Gesichtserkennung ausdrücklich: „A facial recognition match does not establish probable cause to arrest or obtain a search warrant, but serves as a lead for additional investigative steps."[986]

Aber selbst wenn die Polizeibehörden erklären, dass Gesichtserkennungstreffer nicht als alleinige Grundlage für eine Festnahme verwendet werden, bleibt die Frage, welche Maßnahmen als „zusätzliche Ermittlungsschritte" („additional investigative steps") gelten. In der Praxis der US-amerikanischen Strafverfolgungsbehörden scheinen diese weiteren Schritte oft

983 *General/Sarlin*, CNN Business v. 29.4.2021, https://perma.cc/9PT6-HKD8. Ein Richter des Municipal Court unterzeichnete den Haftbefehl und hielt den Gesichtserkennungstreffer daher offenbar auch für ausreichend.

984 Hierzu auch *Benedict*, Washington & Lee Law Review 2022, 849, der einen Vergleich zur Rechtsprechung mit Blick auf Drogenspürhunde vornimmt und argumentiert, dass aufgrund der fehlenden Genauigkeit der Gesichtserkennung ein Treffer nicht die einzige Basis für hinreichende Verdachtsmomente (Probable cause) sein darf.

985 Dies gilt jedenfalls für die Behörden, die ihre Richtlinien zur Gesichtserkennung veröffentlicht haben. 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.". Die Polizeibehörde von Woodbridge (und die Staatsanwaltschaft von Middlesex), die für die Festnahme von Parks verantwortlich waren und offenbar einen Gesichtserkennungstreffer als einzige Grundlage zuließen, äußerten sich nicht auf die Frage von CNN, ob dies noch immer ihre Praxis sei, *General/Sarlin*, CNN Business v. 29.4.2021, https://perma.cc/9PT6-HKD8.

986 NYPD, Questions and Answers Facial Recognition, https://perma.cc/S7YN-8H52.

als erfüllt zu gelten, wenn ein weiterer Mensch den Treffer bestätigt. Verfahrensakten zufolge schickte beispielsweise ein Polizist des NYPD lediglich ein einziges Foto eines Treffers an einen Zeugen und fragte: „Is this the guy […]?".[987] Der Zeuge bejahte die Frage und die Polizei nahm den Mann fest.[988] Mit Blick auf die Überzeugungsbildung im Rahmen der Hauptverhandlung (§ 261 StPO) hat der BGH zu Recht festgestellt, dass bei einer (vorschriftswidrigen) Einzelgegenüberstellung einer Wiedererkennung durch den Zeugen ein wesentlich geringerer Beweiswert zukommt als bei einer vorschriftsmäßigen Wahlgegenüberstellung.[989]

Im Fall von Williams schickte der Gesichtsprüfer (Facial examiner) den Treffer in einem Bericht an die Polizei von Detroit, in dem in fetten Großbuchstaben am oberen Rand stand: „This document is not a positive identification" und „It is an investigative lead only and is not probable cause for arrest".[990] Dem Polizeibericht zufolge erstellten die Ermittler daraufhin eine Wahllichtbildvorlage mit sechs Bildern, darunter eines von Williams. Die Bilder legte die Polizei nicht den Mitarbeitern des Geschäfts vor, in dem der Diebstahl stattgefunden hatte, sondern der Mitarbeiterin eines Geschäftspartners zur Schadensverhütung, die das Überwachungsvideo durchgesehen und auf diesem den Diebstahl entdeckt hatte.[991] Sie identifizierte Mr. Williams als den Dieb auf dem Video. Es bleibt jedoch unklar, was sie für eine solche Identifizierung qualifizierte: Sie war weder eine Augenzeugin noch besonders in Gesichtserkennung geschult. Der Bürgermeister von Detroit räumte ein, dass dies eine „unterdurchschnittliche" („subpar") Polizeiarbeit gewesen war.[992] Dabei hatte er noch nicht einmal berücksichtigt, dass zur Identifizierung nur ein unscharfes Bild des Verdächtigen vorlag.

987 Facial Recognition Motion (redigierte Version) v. 13.11.2019, National Association of Criminal Defense Lawyers, https://perma.cc/VMF4-DFEZ.
988 *General/Sarlin*, CNN Business v. 29.4.2021, https://perma.cc/9PT6-HKD8.
989 BGH, NStZ 1982, 342; NStZ-RR 2017, 90; OLG Koblenz, StV 2007, 348.
990 *Hill*, The New York Times v. 3.8.2020, https://perma.cc/QUF9-RQQF.
991 *Hill*, The New York Times v. 3.8.2020, https://perma.cc/QUF9-RQQF.
992 *Hill*, The New York Times v. 3.8.2020, https://perma.cc/QUF9-RQQF.

f) Wahllichtbildvorlagen

Die oben erwähnte begrenzte menschliche Fähigkeit zur Gesichtserkennung[993] hat auch Bedeutung für Wahllichtbildvorlagen, die ordnungsgemäß erfolgen. Für das deutsche Recht sieht Nr. 18 RiStBV etwa vor, dass dem Zeugen mindestens acht Personen gezeigt werden sollen.[994] Für den Beweiswert einer Wiedererkennung durch einen Zeugen ist nach der Rechtsprechung des BGH die ordnungsgemäße Durchführung der Wahllichtbildvorlage von entscheidender Bedeutung. Erforderlich ist neben einer Anzahl von mindestens acht Vergleichspersonen auch, dass die Lichtbilder einzeln nacheinander vorgelegt werden (sog. sequenzielle Wahllichtbildvorlage).[995] Auch wenn der Zeuge der Auffassung ist, den Täter bereits erkannt zu haben, sind alle Bilder vorzulegen.[996] Die Ermittlungsbehörden haben bei Wahllichtbildvorlagen zudem alles zu unterlassen, was den Zeugen in seiner Unvoreingenommenheit beeinflussen könnte, etwa Kommentare des Vernehmungsbeamten oder besonderes Hinweisen auf das Lichtbild des Verdächtigen.[997] Dennoch kommt es auch bei ordnungsgemäß durchgeführten Wahllichtbildvorlagen zu Fehlidentifizierungen.[998]

Durch den Einsatz von Gesichtserkennung kann es zu noch mehr Fehlern kommen, denn die Technologie ist besonders gut darin, sehr ähnlich aussehende Personen zu finden. Wenn sich der Täter beispielsweise nicht in der durchsuchten Datenbank befindet, stattdessen aber eine andere ihm stark optisch ähnelnde Person, dann ist es für den Zeugen besonders schwierig, zu erkennen, dass es sich nicht um den Täter handelt. Gesichtserkennung birgt daher die Gefahr, dass Fehlidentifizierungen im Rahmen von Wahllichtbildvorlagen noch zunehmen.

993 Vgl. auch *Hofmann*, Personenidentifizierung durch Zeugen im Strafverfahren, 2013, 54 ff.
994 Vgl. auch BGH, NStZ 2012, 172, 173.
995 BGH NStZ 2011, 648 (649) mwN.
996 BGH NStZ 2012, 172 (173).
997 BGH NStZ 2011, 648 (649) mwN.
998 Zu möglichen Faktoren hierfür mit Blick auf den Zeugen, *Hofmann*, Personenidentifizierung durch Zeugen im Strafverfahren, 2013, 66 ff.

g) Fazit zu Fehlern von Menschen

Die Fehler, die im Zusammenhang mit Gesichtserkennung zu den Festnahmen Unschuldiger in den USA geführt haben, sollten nicht schlicht und vorrangig auf schlechte Polizeiarbeit zurückgeführt werden.[999] Es handelt sich nicht nur um einzelne unglückliche Vorfälle, vielmehr bestehen vor allem allgemeine Defizite in der menschlichen Fähigkeit zur Gesichtserkennung, die durch automatisierte Gesichtserkennung noch verstärkt werden.

Die menschliche Fähigkeit zur Gesichtserkennung darf nicht überschätzt werden. Selbst geschulte und beruflich erfahrene Gesichtsprüfer machen regelmäßig Identifizierungsfehler, ähnlich häufig wie ungeschulte Personen. Lediglich bei besonders ausgebildeten Experten kommt es seltener zu Fehlidentifizierungen, aber auch diese sind nicht fehlerfrei. Die menschliche Kontrolle von Gesichtserkennungstreffern kann daher Fehlidentifizierungen und anschließende Ermittlungen gegen Unschuldige nicht ohne Weiteres verhindern.

Es sollte daher gesetzlich festgelegt werden, dass nur besonders ausgebildete Experten mit der Überprüfung von Gesichtserkennungstreffern betraut werden dürfen. Vorgeschrieben werden sollte zudem, dass nur Lichtbilder des Verdächtigen (nicht etwa anderer ähnlich aussehender Personen oder forensische Skizzen) zum Abgleich verwendet werden dürfen.

Allerdings müssen auch die technologischen Entwicklungen im Blick behalten werden. Aus technischer Sicht ist davon auszugehen, dass Gesichtserkennungstechnologien den Menschen in seiner Fähigkeit, Gesichter zu erkennen, *übertreffen* werden (was teilweise ohnehin bereits der Fall ist). Das gilt auch für besonders geschulte Menschen.[1000] Eine zusätzliche „Überprüfung" der Trefferliste durch Menschen würde dann dazu führen, dass es zu *mehr* Fehlern beim Einsatz von automatisierter Gesichtserkennung kommt, wenn Menschen dann häufiger Unschuldige falsch positiv als Verdächtige identifizieren, als dies die Technologie tut.

---

999 Oder auf den Umstand, dass die US-amerikanischen Strafverfolgungsbehörden nicht aktiv entlastende Umstände ermitteln müssen, sondern lediglich ihnen vorliegende entlastende Beweise nicht zurückhalten dürfen, vgl. Brady v. Maryland, 373 U.S. 83 (1963).

1000 In diese Richtung deutet etwa bereits die Untersuchung von *Ramsthaler/Federspiel/Huckenbeck/Kettner/Lux/Verhoff*, Archiv für Kriminologie 2024, Band 254, 1.

3. Fehler in der Mensch-Maschine-Interaktion: Automation bias

Zu den ohnehin begrenzten menschlichen Fähigkeiten zur Gesichtserkennung tritt beim Einsatz automatisierter Gesichtserkennungssysteme noch ein weiteres Problem hinzu: Menschen verlassen sich zu stark auf automatisierte Systeme. Dieses als Automation bias[1001] bezeichnete Phänomen wird verbreitet definiert als die menschliche Tendenz, automatische Hinweise als heuristischen Ersatz für ein aufmerksames Suchen und Verarbeiten von Information zu verwenden.[1002] Entgegenstehende, nicht automatisiert generierte Hinweise werden ignoriert. *Citron* formuliert treffend: „Automation bias effectively turns a computer program's suggested answer into a trusted final decision."[1003] Dass der Automation bias auch beim Einsatz von Gesichtserkennung und Ermittlungen gegen Unschuldige eine Rolle spielt, liegt nahe.[1004]

Auch wenn Gesichtserkennungssysteme typischerweise „nur" eine Kandidatenliste vorschlagen und ein Mensch einen von ihnen als den Verdächtigen auswählt; allein der Umstand, dass die Maschine diesen als Treffer erkannt hat, kann sich auswirken. Dies wäre auch eine mögliche Erklärung dafür, dass Randal Reids Muttermal, Michael Olivers Tattoos, Alonzo Sawyers großer Altersunterschied zum Verdächtigen und Porcha Woodruffs Schwangerschaft die Polizisten nicht daran hinderten, die Betroffenen festzunehmen. Die Tatsache, dass eine Gesichtserkennungstechnologie einen Treffer gefunden hatte, scheint bei ihnen eine vermeintliche Sicherheit hervorgerufen zu haben, die sie davon abhielt, die Übereinstimmung zu

1001 Dazu bereits *Mosier/Skitka*, in: Parasuraman/Mouloua, Automation and Human Performance, 1996, 201; siehe auch *Parasuraman/Riley*, Human Factors 1997, 230; *Skitka/Mosier/Burdick*, International Journal of Human-Computer Studies. 1999, 991, 999; *Cummings*, AIAA 1st Intelligent Systems Technical Conference 2004, 1; *Goddard/Roudsari/Wyatt,* Journal of the American Medical Informatics Association 2012, 121.

1002 *Mosier/Skitka/Burdick/Heers*, Proceedings of the Human Factors and Ergonomics Society Annual Meeting 1996, 204, 205 („the tendency to use automated cues as a heuristic replacement for vigilant information seeking and processing"). Zum Automation bias etwa auch in der rechtswissenschaftlichen Literatur *Sommerer*, Personenbezogenes Predictive Policing, 2020, 71 ff., 330; vgl. auch *Hilgendorf*, in: Fischer, Beweis, 2019, 229, 246.

1003 *Citron*, Washington University Law Review 2008, 1249, 1272.

1004 *Benedict*, Washington & Lee Law Review 2022, 849, 860; *Barrett*, Boston University Journal of Science and Technology Law 2020, 223, 245.

hinterfragen.[1005] Darauf deutet auch die Äußerung des einen Polizisten hin, nachdem er feststellte, dass Robert Williams die falsche Person war: „I guess the computer got it wrong".[1006] Die eigene Verantwortung wird übersehen.

Die Forschung zum Automation bias legt nahe, dass das Risiko einer solchen Voreingenommenheit abnimmt, wenn den Nutzern eines automatisierten Systems eine Dokumentation über die Funktionsweise einer Technologie (Regeln, nach denen sie eine Vorhersage trifft) zur Verfügung gestellt wird und wenn sie darin geschult werden, die Grenzen und die Logik der Technologie zu verstehen.[1007] Dafür dürfte es nicht ausreichend sein, wenn – wie in Deutschland und in den USA praktiziert – der Identifizierungsbericht lediglich darauf hinweist, dass es sich nur um einen „Ermittlungshinweis" handelt. Im Fall von Robert Williams beispielsweise hatte der Gesichtsprüfer, wie oben erwähnt, den Treffer in einer Datei an die Polizei von Detroit geschickt, in der in fetten Großbuchstaben am Anfang stand: „This document is not a positive identification" und „It is an investigative lead only and is not probable cause for arrest".[1008] Dennoch scheint der ermittelnde Polizist den Treffer (neben einer „Identifizierung" durch eine Person, die nicht Augenzeugin war) als hinreichenden Verdacht für eine Festnahme angesehen zu haben. Der bloße Hinweis, dass es sich bei dem Treffer nur um einen Ermittlungshinweis handelt, ersetzt keine umfassende Schulung der Polizisten und zeigt ihnen nicht, wie Gesichtserkennung funktioniert. Er reicht daher nicht aus, um einen Automation bias zu verhindern.

Automation bias kann auch Augenzeugen beeinflussen.[1009] Identifizierungen durch Augenzeugen sind ohnehin bereits nicht das zuverlässigste Beweismittel.[1010] Der BGH beanstandet es nicht, wenn ein Zeuge, sei es

1005 So auch *Ferguson*, Minnesota Law Review 2021, 1105, 1170 („While police would be wise to never solely rely on the technology, the ease of use and the perceived technical precision might overcome common sense human judgment.").

1006 *Benedict*, Washington & Lee Law Review 2022, 849, 861.

1007 *Goddard/Roudsari/Wyatt,* Journal of the American Medical Informatics Association 2012, 121, 123.

1008 *Hill*, The New York Times v. 3.8.2020, https://perma.cc/QUF9-RQQF.

1009 Dies könnte der Grund dafür gewesen sein, dass ein Augenzeuge Michael Oliver trotz seiner Tätowierungen (die der eigentliche Täter nicht hatte) falsch identifizierte, siehe auch *Benedict*, Washington & Lee Law Review 2022, 849, 862.

1010 *National Research Council*, Identifying the Culprit, 2014, 2 („[C]aution must be exercised when utilizing eyewitness procedures and when relying on eyewitness identifications in a judicial context."); United States v. Wade, 388 U.S. 218, 228

mit oder ohne eine entsprechende Information, weiß oder jedenfalls davon ausgeht, dass sich unter den Auswahlpersonen auch die Person des Tatverdächtigen befindet.[1011] Dies erscheint an sich bereits fraglich, denn Studien zeigen, dass die Information an einen Augenzeugen, dass der Täter bei einer Gegenüberstellung anwesend sein könnte, die Wahrscheinlichkeit erhöht, dass sie eine Person auswählen (selbst wenn der Täter nicht dabei ist); auch erhöht dieser Hinweis das Vertrauen der Augenzeugen in ihre Auswahl, selbst wenn diese falsch ist.[1012] Wenn bei einer Wahllichtbildvorlage (oder einer Gegenüberstellung) dem Augenzeugen nun zudem noch mitgeteilt würde, dass der Verdächtige durch automatisierte Gesichtserkennung identifiziert wurde, dürfte es noch wahrscheinlicher sein, dass er einen der „Verdächtigen" identifiziert, selbst wenn dieser nicht der wirkliche Täter ist.[1013] Wenn dann sowohl die Maschine als auch ein Mensch den Verdächtigen als Täter identifiziert haben, könnte dies den ermittelnden Polizisten überdies ein falsches Gefühl von Sicherheit vermitteln.

III. Fazit

Der Einsatz automatisierter Gesichtserkennung kann Folgen – insbesondere Ermittlungsmaßnahmen – für gänzlich Unbeteiligte mit sich bringen. Die Ursache hierfür liegt sowohl in Fehlern der Technologie als auch in menschlichen Fehlern, die durch die Mensch-Maschine-Interaktion noch verstärkt werden. Diese Tatsache muss bei einer Regulierung von Gesichtserkennung berücksichtigt werden, um solche Fälle so weit wie möglich

(1967) („The annals of criminal law are rife with instances of mistaken identification."); siehe auch grundlegend *Borchard*, Convicting the Innocent, 1932 (mit zahlreichen Beispielen von Fehlern von Augenzeugen).

1011 Vgl. zur Wahlgegenüberstellung BGH, NStZ 2011, 648 (649) („Beweiswert nicht schon dadurch gemindert oder in Frage gestellt"), dazu kritisch *Odenthal* StV 2012, 683 (685). Siehe auch MüKoStPO/*Bartel*, 2. Aufl. 2024, StPO § 261 Rn. 280. Siehe für die USA *Garrett*, Columbia Law Review 2008, 55, 60; *Albright/Garrett*, Boston University Law Review 2022, 511.

1012 *Wells/Kovera/Douglass/Brewer/Meissner/Wixted*, Law and Human Behavior 2020, 3, 6, 8 f., 21 f.

1013 Siehe auch *Moy*, William & Mary Bill of Rights Journal 2021, 337, 360 („Because people often trust computer systems as infallible, an eyewitness who knows that automated face recognition was used to try to find the culprit may interpret this information to mean that any identification procedure in which the eyewitness subsequently is asked to participate is likely to include the culprit.").

zu verhindern. Aus technologischer Sicht sollten nur Gesichtserkennungssysteme zum Einsatz kommen, die dem aktuellen Stand der Technik entsprechen. Mit der Überprüfung der Gesichtserkennungstreffer sollten nur besonders ausgebildete Experten betraut werden; zudem sollte verpflichtend ein 4-Augen-Vergleich bei der Überprüfung angeordnet werden. (Wie bereits erwähnt, wird sich in Zukunft allerdings die Frage stellen, was überhaupt der Mehrwert einer menschlichen Überprüfung ist, wenn – was zu erwarten ist – Gesichtserkennungstechnologien auch geschulten Menschen überlegen sind und diese daher *weniger* Fehler machen und damit *seltener* zu Ermittlungen gegen Unschuldige führen als dies bei der Auswahl durch Menschen der Fall wäre.)[1014] Auch könnte – zumindest in internen Leitlinien – festgelegt werden, dass die Erkennung nicht durch den Ermittler erfolgen darf, der mit dem Fall befasst und daher womöglich voreingenommen ist und vorschnell zumindest einen Verdacht auf Personenidentität bejahen könnte, um einen Ermittlungsansatz zu haben.[1015] Zudem muss sichergestellt sein, dass nur Lichtbilder des Verdächtigen zum Abgleich verwendet werden. Bei einer Wahllichtbildvorlage oder Gegenüberstellung muss gewährleistet sein, dass dem Zeugen nicht offenbart wird, dass Gesichtserkennung verwendet wurde. Die Ermittler bei der Polizei werden, soweit ersichtlich, derzeit nicht darin geschult, wie automatisierte Gesichtserkennung funktioniert; dies sollte zukünftig geändert werden, um einem Automation bias entgegenzuwirken.

Diese Erkenntnisse verdeutlichen erneut die Notwendigkeit einer – auch bereits verfassungsrechtlich fundierten – Pflicht zur Benachrichtigung des Beschuldigten über den Gesichtserkennungseinsatz. Der Beschuldigte und sein Verteidiger sind dadurch gewarnt, dass eine besonders fehleranfällige Technologie verwendet wurde und können hierauf im Ermittlungs- und Gerichtsverfahren hinweisen. Zudem wird erneut deutlich, dass eine umfassende Evaluation der Verwendung von Gesichtserkennung in der Strafverfolgung erfolgen muss. Nur wenn die Fälle, in denen die Technologie verwendet wurde, systematisch nachverfolgt und ausgewertet werden, kann Fehlentwicklungen vorgebeugt werden. Dies geschieht aber derzeit nicht. Wie bereits oben angesprochen,[1016] wird hier eine Kontrolle allein durch einen Datenschutzbeauftragten nicht zielführend sein; die Evaluation muss

1014 Siehe aber zu Folgefragen Kapitel IV. C. IV.

1015 Dies dürfte zwar regelmäßig bereits gewährleistet sein, wenn die Identifizierung durch einen Lichtbildexperten oder -sachverständigen erfolgt; gleichwohl erscheint eine ausdrückliche Regelung aber sinnvoll.

1016 Kapitel II. A. 3. c) cc).

umfassender sein. Um eine solche zu ermöglichen, ist eine Dokumentationspflicht für den Einsatz von Gesichtserkennung vorzusehen. Diese Evaluation kann wiederum zur Schulung von Polizisten verwendet werden, um für Probleme zu sensibilisieren.

C. Mediale Darstellung des Einsatzes von Gesichtserkennung

I. Ausgangspunkt und Forschungsfragen

Automatisierte Gesichtserkennung wird wie kaum eine andere Strafverfolgungstechnologie – abgesehen von der Vorratsdatenspeicherung und der sog. „Chatkontrolle" – in den Medien und in der Öffentlichkeit diskutiert. Die Verwendung der Technologie in der Strafverfolgung könnte sich daher auch darauf auswirken, wie die Arbeit der Polizei und des Staates als Ganzes wahrgenommen werden.[1017] Staatliches und insbesondere polizeiliches Handeln lebt von gesellschaftlicher Akzeptanz. Zwar zeigen Studien grundsätzlich eine Zufriedenheit der Bevölkerung mit der Polizei.[1018] Dabei wird jedoch nur die „analoge" Polizeiarbeit untersucht, nicht speziell wie der Einsatz neuer Technologien wahrgenommen wird. Durch den Einsatz neuer Strafverfolgungstechnologien wird das Vertrauen in die Polizei auf den Prüfstand gestellt, zumal wenn diese – wie die Gesichtserkennung – mit Künstlicher Intelligenz und Diskriminierung in Zusammenhang gebracht werden. Dies gilt insbesondere vor dem Hintergrund, dass über 70 % der Bevölkerung der Ansicht sind, die Politik unternehme nicht genug gegen mögliche Risiken von KI[1019] und viele insbesondere Angst vor einer „flächendeckenden Überwachung" äußern.[1020] Wenn die Bevölkerung den Einsatz automatisierter Gesichtserkennung als problematisch ansieht, droht das Vertrauen in die Polizei zu sinken.[1021]

Kostka, *Steinacker* und *Meckel* zeigen in ihrer Studie zur Akzeptanz staatlichen und nichtstaatlichen Einsatzes von Gesichtserkennungstechnologien

1017 In eine ähnliche Richtung mit Blick auf personenbezogenes Predictive Policing *Sommerer*, Personenbezogenes Predictive Policing, 2020, 305 ff.; vgl. auch *Bragias/Hine/Fleet*, Police Practice and Research 2021, 1637, 1637 f.

1018 Siehe nur *Birkel/Church/Erdmann/Hager/Leitgöb-Guzy*, Sicherheit und Kriminalität in Deutschland, 2020, 158 ff.

1019 *Fox/Privitera/Reuel*, KIRA Report, 2023, 6.

1020 *Fox/Privitera/Reuel*, KIRA Report, 2023, 4.

1021 *Bragias/Hine/Fleet*, Police Practice and Research 2021, 1637, 1637 f.

im öffentlichen Raum, unter anderem in Deutschland, dass im Hinblick auf den Einsatz von Gesichtserkennung Bedenken bestehen.[1022] Sie bleiben hier allerdings sehr allgemein („privacy violation", „discrimination", „surveillance").[1023]

Um diese Vorbehalte und die Einstellung der Bevölkerung zu Gesichtserkennung besser untersuchen, nachvollziehen und einordnen zu können, erscheint es sinnvoll, zunächst kriminologisch-sozialwissenschaftlich zu analysieren, wie Gesichtserkennung *in den Medien* dargestellt wird. Dieses Ziel verfolgte die vorliegende Studie. Ein solches Vorgehen erscheint bereits deshalb angezeigt, weil vergangene Bevölkerungsbefragungen zur Einstellung gegenüber Gesichtserkennung den Eindruck nahelegten, dass ein signifikanter Anteil der Befragten trotz Erklärung Gesichtserkennung missverstehen. In einer von *Kostka/Steinacker/Meckel* im Jahr 2021 durchgeführten Studie antwortete beispielsweise ein Fünftel der befragten Deutschen, dass sie schon einmal ein Gesichtserkennungssystem in öffentlichen Straßen oder Bahnhöfen gesehen hätten.[1024] Da jedoch zuletzt lediglich die Bundespolizei in den Jahren 2017/2018 biometrische Gesichtserkennung am Bahnhof Berlin Südkreuz testete,[1025] deutet diese Antwort eher darauf hin, dass die Befragten normale Videokameras für Gesichtserkennungssysteme hielten.[1026]

Zudem ist davon auszugehen, dass die mediale Darstellung der Technologie zumindest mitbeeinflusst, wie die Bevölkerung den Einsatz automatisierter Gesichtserkennung in der Strafverfolgung wahrnimmt und in Zukunft wahrnehmen wird. *Luhmanns* Ausspruch „Was wir über unsere Gesellschaft wissen, ja über die Welt, in der wir leben, wissen wir

1022 *Kostka/Steinacker/Meckel*, Public Understanding of Science 2021, 671.
1023 *Kostka/Steinacker/Meckel*, Public Understanding of Science 2021, 671, 684.
1024 *Kostka/Steinacker/Meckel*, Public Understanding of Science 2021, 671, 686.
1025 *Bundespolizei*, Teilprojekt 1 „Biometrische Gesichtserkennung" des Bundespolizeipräsidiums im Rahmen der Erprobung von Systemen zur intelligenten Videoanalyse durch das Bundesministerium des Innern, für Bau und Heimat, das Bundespolizeipräsidium, das Bundeskriminalamt und die Deutsche Bahn AG am Bahnhof Berlin Südkreuz im Zeitraum vom 01.08.2017 - 31.07.2018, 2018.
1026 *Kostka/Steinacker/Meckel*, Public Understanding of Science 2021, 671, 686: „For instance, one fifth of the German respondents reported seeing FRT in public streets and railway stations. But given that by 2019, only the train station Berlin Südkreuz had experimented with FRT, and despite the survey's introductory disclaimer explaining what we mean by ‚FRT', some respondents confuse standard video cameras with the more advanced FRT software behind them."

durch die Medien“[1027] mag überspitzt sein;[1028] für das Thema der Gesichtserkennung scheint dies aber nicht abwegig. Da diese Technologie erst in den letzten Jahren bekannter wurde, liegt es nahe, dass das Wissen der meisten Menschen über die Gesichtserkennung vorrangig aus Filmen (etwa „Minority Report“ oder „The Circle“) oder Medienberichten stammt. Ob und wie stark die Medien nicht nur das Wissen, sondern auch die Einstellung der Bevölkerung beeinflussen, hängt zwar von vielen Faktoren ab.[1029] Mediale Beiträge haben aber jedenfalls das Potenzial, die Einstellung von Menschen zu beeinflussen, sie entweder zu verstärken oder zu ändern.[1030] Eine jüngere Studie zeigt etwa, dass im Rahmen medialer Berichterstattung das Framing (Einrahmen) von KI als Chance oder als Risiko eine emotionale Wirkung hat und so die Einstellungen gegenüber KI beeinflusst;[1031] insbesondere erhöhen Risiko-Frames die Sorge von Menschen vor KI.[1032]

Folgende Forschungsfragen werden untersucht:

- Welches Bild zeichnen die Medien von automatisierter Gesichtserkennung als Strafverfolgungstechnologie?
- Welche Themen sind häufig Gegenstand der Berichterstattung?
- Welche Bedenken oder Risiken werden erwähnt?

II. Methodik: Qualitative Inhaltsanalyse von Medienbeiträgen

Um sich der Frage anzunähern, welches Bild vom Einsatz automatisierter Gesichtserkennung in der Strafverfolgung in den Medien gezeichnet wird, wurde eine qualitative Inhaltsanalyse von Medienbeiträgen durchgeführt.

1027 *Luhmann*, Die Realität der Massenmedien, 2017, 9.
1028 Zur Kritik etwa *Reichertz*, Die Macht der Worte und der Medien, 2009, 17 f.
1029 Vgl. nur zu den Faktoren für eine Einstellungsänderung *Bonfadelli/Friemel*, Medienwirkungsforschung, 2017, 139 ff; *Schenk*, Medienwirkungsforschung, 2007, 85 ff.
1030 Vgl. etwa *Coppock/Ekins/Kirby*, Quarterly Journal of Political Science 2018, 59. *Baum/Potter*, Annual Review of Political Science 2008, 39; beispielhaft auch *Huang/Cook/Xie*, Humanities and Social Sciences Communications 2021, 1. Zu möglichen Wirkmechanismen *Bonfadelli/Friemel*, Medienwirkungsforschung, 2017, 161 ff. Im Einzelnen ist jedoch umstritten, inwieweit und auf welche Weise Medien die öffentliche Meinungsbildung beeinflussen und welche weiteren Faktoren auf die Meinungsbildung wirken.
1031 *Fucker*, in: van Oorschot/Fucker, Framing KI, 2022, 81, 103 f.
1032 *Fucker*, in: van Oorschot/Fucker, Framing KI, 2022, 81, 104.

1. Wahl der Methodik

Empirische Sozialforschung dient dazu, möglichst zutreffende Aussagen über die soziale Lebenswirklichkeit zu treffen und zu diesem Zweck Hypothesen zu entwickeln oder zu überprüfen. Während das vorrangige Ziel quantitativer Forschung darin besteht, soziale Phänomene messbar zu machen und statistisch auszuwerten sowie Hypothesen und Theorien zu überprüfen,[1033] zeichnet sich qualitative Forschung dadurch aus, dass sie vorrangig darauf ausgerichtet ist, Hypothesen zu generieren[1034].[1035] Ein qualitativer Forschungsansatz wurde deshalb gewählt, weil es sich bei der automatisierten Gesichtserkennung um eine so neue Technologie handelt, dass noch nicht genügend Erkenntnisse vorhanden sind, um Theorien zu der Einstellung der Bevölkerung in diesem Bereich zu bilden.[1036] Zudem bestand das Ziel der Studie darin, mögliche Bedenken inhaltlich zu verstehen; dafür eignen sich qualitative Ansätze, da diese mehr auf Tiefe als auf Breite angelegt sind.

Um die Forschungsfragen zu beantworten, wurde eine qualitative Inhaltsanalyse von Medienbeiträgen durchgeführt. Qualitative Inhaltsanalysen[1037] zielen darauf ab, fixierte Kommunikation (z. B. Texte) unter einer theoretisch ausgewiesenen Fragestellung systematisch und regelgeleitet zu untersuchen und daraus Rückschlüsse zu ziehen.[1038] Als Gegenstand der

1033 Vgl. nur *Häder*, Empirische Sozialforschung, 2015, 64; siehe aber zur Möglichkeit der Überprüfung von Hypothesen mit qualitativer Forschung etwa *Mayring*, Qualitative Inhaltsanalyse: Grundlagen und Techniken, 2022, 25.

1034 *Mayring*, Qualitative Inhaltsanalyse, 2022, 22 f.; *Strauss/Corbin*, Grounded Theory, 1996, 7 ff.

1035 Die Abgrenzung zwischen quantitativer und qualitativer Forschung ist allerdings nicht immer trennscharf, außerdem können beide Ansätze mit einem Mixed-Methods-Ansatz verknüpft werden, siehe nur *Kuckartz*, Mixed Methods, 2014, 33, 52 ff; *Steger*, Einführung in die qualitative Sozialforschung, 2003, 3. Kritisch zur strikten Trennung („Dichotomisierung") quantitativer und qualitativer Forschung bereits *v. Saldern*, Empirische Pädagogik 1992, 377; siehe auch *Häder*, Empirische Sozialforschung, 2015, 61.

1036 Zur Offenheit der qualitativen Methoden *Steger*, Einführung in die qualitative Sozialforschung, 2003, 4.

1037 Begriff und Ansatz gehen zurück auf *Kracauer*, The Public Opinion Quarterly 1952, 631 (Qualitative content analysis).

1038 *Mayring*, Qualitative Inhaltsanalyse, 2022, 12 f.; zu verschiedenen Varianten der qualitativen Inhaltsanalyse *Schreier*, Forum Qualitative Sozialforschung/Forum Qualitative Social Research 2014, 1; siehe zur Inhaltsanalyse auch *Dölling/Hermann/Laue*, Kriminologie, 2022, § 3 Rn. 12; vgl. auch *Meuser*, in: Bohnsack/Geimer/Meuser, Hauptbegriffe qualitativer Sozialforschung, 2018, 120, 121.

Analyse wurden Medienbeiträge gewählt, da die Darstellung von Gesichtserkennung in den Medien untersucht werden sollte.

2. Auswahl der Beiträge

Für die Untersuchung wurden zunächst online verfügbare Medienberichte aus den Jahren 2018 bis 2023 recherchiert, die den Einsatz automatisierter Gesichtserkennung in der Strafverfolgung zum Gegenstand haben. Nicht einbezogen wurden Berichte über den Einsatz sog. (menschlicher) Super-Recognizer, die nur am Rande die automatisierte Gesichtserkennung erwähnen. Es wurden ausschließlich deutsche Medien berücksichtigt, deutschsprachige Beiträge von österreichischen oder schweizerischen Medien hingegen nicht. Private Blogeinträge wurden nicht einbezogen. Recherchiert wurden Artikel, die im Zeitraum vom 1.1.2018 bis zum 31.8.2023 erschienen sind. Dieser Eingrenzung lag zugrunde, dass dieser Berichtszeitraum einerseits groß genug erscheint, um nicht von einzelnen Vorkommnissen monopolisiert zu werden, etwa den Tests von Gesichtserkennung am Bahnhof Berlin/Südkreuz in den Jahren 2017/2018 oder der Enthüllung der Tätigkeit von *Clearview AI* durch die New York Times Reporterin Kashmir Hill im Jahr 2020. Andererseits stellt die Beschränkung die Durchführbarkeit der Studie und die Aktualität der Ergebnisse sicher.

Aus dem Pool all dieser Berichte wurden im nächsten Schritt die inhaltlich zu untersuchenden Beiträge ausgewählt. Qualitative Forschung erhebt nicht den Anspruch auf Repräsentativität im statistischen Sinne, sondern auf eine phänomenologische Repräsentation sozialer Wirklichkeiten. Es soll sichergestellt werden, dass ein Phänomen in seinen verschiedenen Ausprägungen erfasst wird. Um eine Verallgemeinerbarkeit der Ergebnisse zu ermöglichen, ist vor allem das Sampling entscheidend, also die Auswahl der Fälle (hier: Medienbeiträge).[1039] Für diese Studie erschien eine Kombination aus kriteriengeleitetem Sampling im ersten Schritt und Zufallsauswahl im zweiten Schritt sachgerecht. Bei der Strategie des kriteriengeleiteten Sampling werden die Merkmale für das Sampling bereits vor der Erhebung identifiziert.[1040] Dann werden aus dem Pool gezielt Fälle, also hier Medienbeiträge, in das Sample einbezogen, die die Heterogenität des Untersuchungsfeldes repräsentieren. Dieses Vorgehen bietet sich an,

1039 *Przyborski/Wohlrab-Sahr*, Qualitative Sozialforschung, 2021, 227 f., 447, 453.
1040 Vgl. *Przyborski/Wohlrab-Sahr*, Qualitative Sozialforschung, 2021, 233 ff.

wenn bereits theoretisches oder empirisches Wissen über mögliche Strukturierungsmerkmale vorliegt. Für die vorliegende Studie war insbesondere darauf zu achten, dass Berichte verschiedener Medienorgane einbezogen werden. Daher wurden die Beiträge in drei Kategorien unterteilt: (1) reichweitenstarke überregionale Zeitungen und Magazine, (2) Online-Medienportale und Online-Magazine, (3) regionale/lokale Zeitungen. Im zweiten Schritt wurden dann per Zufallsauswahl aus den ersten beiden Kategorien 15 Beiträge, aus der dritten 8 Beiträge ausgewählt. Es wurde lediglich sichergestellt, dass Medienorgane unterschiedlicher politischer Ausrichtung vertreten waren. Zugelassen wurde aber, wenn mehrere Beiträge von demselben Medienorgan stammten. Insgesamt wurden daher 38 Medienbeiträge in die qualitative Inhaltsanalyse einbezogen.[1041] Für die Auswertung und die Darstellung der Ergebnisse wurde jedem dieser Beiträge eine Referenznummer zugeordnet (Beitrag 1, Beitrag 2, …).

3. Vorgehen bei der Analyse

Die Beiträge wurden anhand einer inhaltlich strukturierenden qualitativen Inhaltsanalyse in Anlehnung an *Kuckartz*[1042] ausgewertet. Teilweise wurde diese kombiniert mit Elementen der evaluativen (bewertenden) Inhaltsanalyse;[1043] es wurden für einzelne besonders interessierende Bereiche evaluative Kategorien definiert.[1044] Durch das regelgeleitete Vorgehen sollte sichergestellt werden, dass die Ergebnisse intersubjektiv nachvollziehbar sind.

Zunächst wurden ausgehend von den Forschungsfragen alle Texte Abschnitt für Abschnitt anhand von groben Hauptkategorien durchgesehen und zugeordnet (codiert). Angesichts der Offenheit der qualitativen Methode ergaben sich hierbei einerseits Änderungen in Zuschnitt und Formu-

1041 Die Beiträge stammten aus folgenden Medien: Süddeutsche Zeitung, Rheinische Post, BuzzFeed, Münchner Merkur, ProSieben Newstime, Focus, DIE ZEIT, heise, WAZ, Münstersche Zeitung, Frankfurter Rundschau, Hamburger Abendblatt, Badische Zeitung, Stern, Spiegel, Bayerischer Rundfunk, Welt, MDR, Deutschlandfunk Kultur, BILD, t3n, The Decoder, Redaktionsnetzwerk Deutschland, Handelsblatt, Taz, ZDNet, Netzpolitik.org.

1042 *Kuckartz*, Qualitative Inhaltsanalyse, 2018, 97 ff; vgl. auch *Steger*, Einführung in die qualitative Sozialforschung, 2003, 14.

1043 Zu dieser *Kuckartz*, Qualitative Inhaltsanalyse, 2018, 123 ff.

1044 Zur Möglichkeit der Kombination auch *Kuckartz*, Qualitative Inhaltsanalyse, 2018, 141.

lierung der Kategorien und andererseits weitere, nicht erwartete Kategorien. Nach diesem ersten Codierprozess wurden im nächsten Schritt alle Textstellen einer Kategorie zusammengetragen und dann innerhalb dieser Kategorien differenziertere Subkategorien gebildet.[1045] Bei diesen Subkategorien handelte es sich teilweise um evaluative Kategorien, also solche, die eine Wertung erforderlich machten. Eine Textstelle konnte auch mehreren Kategorien oder Subkategorien zugeordnet werden.[1046] Anschließend wurde in einem zweiten Codierprozess das komplette Material anhand der ausdifferenzierten Subkategorien codiert.[1047] Zum Beispiel lautete eine (Haupt-)Kategorie „Darstellung der Fehleranfälligkeit der Technologie", als eine Subkategorie kristallisierte sich beispielsweise „Hohe Fehlerquoten" heraus. Die Darstellung der Ergebnisse orientiert sich an diesen Kategorien und Subkategorien.

Als qualitative Inhaltsanalyse erhebt diese Untersuchung keinen Anspruch auf Repräsentativität in einem quantitativen (statistischen) Sinne. Dennoch ist sie geeignet, einen Eindruck davon zu vermitteln, wie der Einsatz automatisierter Gesichtserkennung in der Strafverfolgung in den Medien dargestellt wird.

III. Ergebnisse

1. Unterscheidung von Einsatzszenarien

Allgemein fällt auf, dass viele Beiträge nicht zwischen den verschiedenen Einsatzmöglichkeiten von Gesichtserkennung unterscheiden. Unter dem Schlagwort „Gesichtserkennung" werden unterschiedliche Anwendungsfälle aufgezählt.

> *„Weltweit ist Gesichtserkennung auf dem Vormarsch. Russland identifiziert damit Demonstranten. Pornhub erkennt Darstellerinnen in hochgeladenen Videos. Frankreich will allen Bürgern eine ‚digitale Identität' geben, die an ihr Gesicht geknüpft ist. Und China lässt nicht nur Uiguren, sondern einen Großteil der Bevölkerung mit Kameras überwachen. Auch in Deutschland*

1045 Dies erfolgte anhand des Textmaterials, was von *Kuckartz* in diesem Zusammenhang als induktives Vorgehen bezeichnet, *Kuckartz*, Qualitative Inhaltsanalyse, 2018, 72 f.

1046 Vgl. hierzu auch *Kuckartz*, Qualitative Inhaltsanalyse, 2018, 102 f.

1047 *Kuckartz*, Qualitative Inhaltsanalyse, 2018, 110 f.

will Innenminister Seehofer die Gesichtserkennung im öffentlichen Raum massiv ausweiten.“ (Beitrag 18)

Dabei werden Einsatzszenarien Privater und der Polizei häufig in einem Atemzug genannt, ohne sie näher zu beschreiben.

„Die Fußball-Bundesliga setzt seit Anfang des Jahres das System ein, um die Aufzeichnungen von Spielen zu organisieren. Fans könnten dann alle Spielszenen einer Saison nach ihrem Lieblingsspieler durchsuchen. Auch Polizeibehörden etwa im US-Bundesstaat Washington setzen das System ein, um Datenbanken mit Überwachungskamera-Aufzeichnungen abzugleichen und so Ladendiebstähle zu verfolgen.“ (Beitrag 37)

Warum hier etwa ausgerechnet Polizeibehörden im US-Bundesstaat Washington erwähnt werden, bleibt unklar. Teilweise wird lediglich zwischen dem Einsatzmodus der Verifizierung/Authentifizierung einerseits und der Identifizierung andererseits unterschieden. Unter Verweis auf eine Interviewpartnerin wird die Verifizierung/Authentifizierung, also der 1:1-Abgleich, als unproblematisch dargestellt:

„‚Der erste Einsatzzweck von Gesichtserkennungstechnologie ist die Authentifizierung, die Sie in der Regel selbst vornehmen: Sie entsperren ihr Smartphone, indem sie Ihr Gesicht mit dem im Telefon gespeicherten Bild abgleichen. Oder Sie identifizieren sich, indem Sie sich an der automatischen Passkontrolle am Flughafen fotografieren lassen und das Bild mit dem in Ihrem Pass verglichen wird‘, erklärt sie.
‚Diese Art der Gesichtserkennung birgt, wenn sie regelkonform vorgenommen wird, nur geringe Risiken. Denn Sie allein haben ja die Kontrolle über das Bild in ihrem Smartphone oder Pass. Da wird nichts mit einer zentralen Datenbank abgeglichen.‘“ (Beitrag 5)

Dem wird die „*biometrische Massenüberwachung*“ gegenübergestellt. Dass neben dem 1:1-Abgleich (Verifizierung/Authentifizierung) auch Anwendungsmöglichkeiten für Gesichtserkennung bestehen, die keine biometrische Massenüberwachung bedeuten, wird nicht erwähnt.

„‚Problematischer sei das zweite Einsatzfeld von Gesichtserkennungstechnologie‘, erklärt Francesco Ragazzi, Professor für Politikwissenschaft an der Universität Leiden und Autor einer Studie zum Thema für das Europäische Parlament.
‚Sucht dieses System eine einzelne Person, indem es die Gesichter von zahllosen Passanten scannt? Oder sucht das System die Person, indem es

> *Videoaufnahmen aus einem Bahnhof oder einem Einkaufszentrum untersucht? In solchen Fällen haben wir es mit Eingriffen ins Privatleben und die Menschenrechte zu tun – mit biometrischer Massenüberwachung.“ (Beitrag 5)*

Auch die verschiedenen Einsatzszenarien im Bereich der Strafverfolgung werden in vielen Beiträgen nicht unterschieden. Ein Beitrag berichtet etwa von dem Einsatz von Gesichtserkennung im öffentlichen Raum in London, China und Indien, im nächsten Satz dann von der Verwendung der Software *Clearview AI* durch US-amerikanische Strafverfolgungsbehörden, die jedoch nicht zur Fahndung im öffentlichen Raum, sondern zur nachträglichen Erkennung Verdächtiger auf Bildmaterial verwendet wird:

> *„Die Londoner Polizei gab am Freitag vergangener Woche bekannt, dass sie die Kameras der Stadt mit einer Gesichtserkennungssoftware und einer Datenbank verknüpfen will. Nach China wäre das Vereinigte Königreich damit der erste Staat, der seine Bürger mit Gesichtserkennung überwacht. Das Prinzip ist weltweit auf dem Vormarsch: Indien plant, ein ähnliches System einzuführen. Erst vergangene Woche war bekannt geworden, dass amerikanische Polizisten schon eine Gesichtserkennungssoftware namens Clearview nutzen – die die notwendigen Bilder von Social-Media-Accounts kopiert.“ (Beitrag 22)*

2. Darstellung des Einsatzes in Deutschland

Rund zwei Drittel der untersuchten Beiträge erwähnen in mehreren Sätzen oder zumindest in einem Satz, dass auch in Deutschland Gesichtserkennung in der Strafverfolgung verwendet wird. Die meisten Artikel berichten über den Einsatz in China und den USA, einige wenige Beiträge befassen sich nur mit dem Einsatz in Deutschland.

a) Differenzierung zwischen Einsatzszenarien

Bei der Darstellung des Einsatzes von Gesichtserkennung in Deutschland zeigt sich ebenfalls, dass zwischen den verschiedenen Szenarien nicht klar unterschieden wird.

Unter der Unterüberschrift *„Gesichtserkennung wird in Deutschland häufig genutzt“* findet sich in einem Beitrag etwa ohne nähere Erläuterung der

Hinweis, dass sich die Nutzung von Gesichtserkennung *„in der INPOL-Datei"* erhöht habe und dass eine Ausweitung der Technologie an Flug- und Bahnhöfen geplant sei. Es wird nicht darauf eingegangen, dass letzteres ein gänzlich anderes Einsatzszenario (Echtzeit-Fahndung im öffentlichen Raum) ist.

> *„Bei der Bundespolizei hat sich die Nutzung der Gesichtserkennung in der INPOL-Datei verdreifacht, Bundesinnenminister Horst Seehofer forderte eine Ausweitung der Technologie und wollte diese an mehr als 100 Flug- und Bahnhöfen einsetzen." (Beitrag 32)*

Ein anderer Beitrag stellt fest, dass *„die automatisierte Gesichtserkennung"* in Deutschland vorerst nicht ausgeweitet werde, ohne näher zu erläutern, von welcher Einsatzvariante die Rede ist (gemeint war wohl auch hier die Echtzeit-Fahndung im öffentlichen Raum). Ab dem nächsten Satz spricht der Beitrag von der Einsatzvariante der Identitätsermittlung, ohne den Unterschied zu der zuvor erwähnten Echtzeit-Fahndung im öffentlichen Raum zu erwähnen.

> *„Bundesinnenminister Horst Seehofer verzichtet vorerst darauf, die automatisierte Gesichtserkennung in Deutschland mithilfe des künftigen Bundespolizeigesetzes auszuweiten. Doch das heißt nicht, dass die Technik an sich hierzulande tabu ist – im Gegenteil. Polizisten in Deutschland finden heute schon Hunderte mutmaßliche Täter per Gesichtserkennungssoftware." (Beitrag 4)*

Was hinter den unterschiedlichen Einsatzvarianten von Gesichtserkennung steht, wird in den meisten Beiträgen nicht näher erläutert; sie werden lediglich aufgezählt.

> *„Das Bundeskriminalamt (BKA) etwa nutzt schon seit 2008 das Gesichtserkennungssystem GES. Die Zahl der damit durchgeführten Recherchen steigt seit Jahren rasant an. 2021 konnten die Beamten so in 90.000 Abfragen rund 5000 Personen identifizieren, nachdem sie die Ergebnisse des Systems händisch verifizierten. Die besonders umkämpfte Echtzeit-Identifizierung soll mit GES nicht stattfinden. Für Proteste von Datenschützern sorgte in den vergangenen Jahren vor allem die Suche der Hamburger Staatsmacht nach Randalierern beim G20-Gipfel per biometrischer Gesichtserkennung." (Beitrag 19)*

Insgesamt vermitteln die Beiträge jeweils ein sehr unterschiedliches Bild vom Einsatz von Gesichtserkennung durch deutsche Strafverfolgungsbe-

hörden. Viele Beiträge erwähnen ausschließlich die Erprobung von Echtzeit-Fahndung am Bahnhof Berlin Südkreuz, einige darüber hinaus die Gesichtserkennungsauswertung durch die Polizei Hamburg nach den Ausschreitungen wegen des G20-Gipfels.

b) Einsatz zur Identifizierung unbekannter Verdächtiger

aa) Seltene Erwähnung

Dass Gesichtserkennung in Deutschland auch verwendet wird, um unbekannte Verdächtige zu identifizieren, berichten viele Beiträge nicht. Ein Artikel berichtet etwa ausführlich über dieses Einsatzszenario in den USA, erwähnt aber nicht, dass ein ähnliches auch in Deutschland Realität ist. Stattdessen wird nur auf die Erprobung von Echtzeit-Gesichtserkennung am Bahnhof Berlin Südkreuz eingegangen.

> *„Auch in Deutschland wird seit Monaten über eine mögliche Einführung von automatischer Gesichtserkennung diskutiert. Ein Pilotprojekt zur Videoüberwachung am Berliner Bahnhof Südkreuz ..." (Beitrag 24)*

Ein anderer Artikel befasst sich im Ausgangspunkt mit der Verwendung von *Clearview AI* durch US-amerikanische Strafverfolgungsbehörden zur Identifizierung unbekannter Verdächtiger. Bei der Darstellung der Situation in Deutschland wird nicht angesprochen, dass Verdächtige anhand einer Recherche in INPOL identifiziert werden können. Der Beitrag erwähnt nur, dass Unternehmen strenge Voraussetzung erfüllen müssen, um biometrische Erkennungsverfahren einzusetzen, und verweist mit Blick auf die Strafverfolgung auch hier nur auf das Pilotprojekt am Bahnhof Berlin Südkreuz:

> *„In Deutschland stellt die Datenschutz-Gesetzgebung an den Einsatz biometrischer Erkennungsverfahren ‚strenge Anforderungen', sagt Marit Hansen vom Landesdatenschutzzentrum Schleswig-Holstein.*
> *Insbesondere Privatanwender und Unternehmen müssen von jeder Person, deren Gesicht sie abgleichen wollen, eine Genehmigung einholen. Die Übermittlung der Daten an Dienstleister im Ausland unterliegt ebenfalls strengen Auflagen. Das macht den Einsatz smarter Überwachungskameras für Privatleute mindestens schwierig.*
> *Ob Behörden die Technik im öffentlichen Raum einsetzen dürfen, ist umstritten: Als die Bundespolizei am Bahnhof Berlin Südkreuz im Jahr*

> *2018 eine Gesichtserkennung ausprobiert hatte, verwies das zuständige Innenministerium auf das Gesetz über die Bundespolizei – zudem könnten Bahnhofsbesucher den gekennzeichneten Kontrollbereich einfach umgehen." (Beitrag 37)*

Dass der in Deutschland bereits praktizierte Einsatz automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger häufig unerwähnt bleibt, macht auch ein besonders ausführlicher Beitrag deutlich. Es wird sowohl auf den Einsatz von Gesichtserkennung in verschiedenen Ländern wie China, Großbritannien und den USA eingegangen, ausführlich auch verschiedene Einsatzvarianten in der Strafverfolgung besprochen und Gefahren der Technologie durch Überwachung und Festnahmen Unbeteiligter erläutert. Mit Blick auf den Einsatz von Gesichtserkennung durch deutsche Strafverfolgungsbehörden bespricht der Beitrag vertieft das Pilotprojekt am Bahnhof Berlin Südkreuz und die Gesichtserkennungsauswertung durch die Hamburger Polizei im Zusammenhang mit den Ausschreitungen wegen des G20-Gipfels. Dass die Technologie auch zur Identifizierung unbekannter Verdächtiger verwendet wird, erwähnt der lange Beitrag in nur zwei Sätzen.

> *„Unter dem Radar der Öffentlichkeit jedoch identifiziert die Polizei längst routinemäßig Straftäter, auch Kleinkriminelle. Die Videoaufnahme zum Beispiel eines Randalierers am Bahnhof wird abgeglichen mit Bildern, über die der Staat verfügt." (Beitrag 5)*

Welche Polizeibehörden unter welchen Voraussetzungen mit welchem Gesichtserkennungssystem und auf welche Weise Verdächtige identifizieren, wird nicht näher erläutert. Das seit 2008 betriebene Gesichtserkennungssystem GES des BKA bleibt ebenso unerwähnt wie der Ablauf solcher Erkennungsvorgänge.

Andere Beiträge erwähnen die Verwendung von Gesichtserkennung zur Identifizierung unbekannter Verdächtiger hingegen, einige wenige befassen sich näher mit der Thematik. Dabei wird vor allem über den Einsatz beim LKA Bayern berichtet, teilweise wird auch das Erkennungssystem des BKA angesprochen.

bb) Zum Abgleich herangezogene Datenbanken

Welche Datenbanken zum Abgleich herangezogen werden dürfen, bleibt meist unerwähnt. Exemplarisch ist der folgende Ausschnitt:

> *„Die Polizei befürwortet andernorts jedoch nach wie vor den Einsatz der Technologie. In Deutschland nutzt das Bundeskriminalamt (BKA) seit 2008 ein Gesichtserkennungssystem (GES) zur Identifizierung unbekannter Täter. Seit 2016 führen BKA, Bundespolizei und die Landespolizeien pro Jahr mehr als 20.000 Recherchen im GES des BKA durch." (Beitrag 16)*

Manche Beiträge sprechen von einem Abgleich mit *„Datenbanken der Polizei" (Beitrag 21, Beitrag 28),* andere berichten, dass Bilder von Verdächtigen *„mit dem Lichtbild-Gesamtbestand im zentralen Informationssystem der Polizei" (Beitrag 30)* abgeglichen werden. Dabei wird nicht ausgeführt, wessen Gesichtsbilder dort gespeichert sind. Ein anderer Beitrag erwähnt die Möglichkeit eines Abgleichs *„mit Fotos aus einer Datenbank des Bundeskriminalamtes (BKA)" (Beitrag 4)*. Der Inhalt der Datenbank wird etwas konkreter umschrieben:

> *„In der sind Bilder von Inhaftierten enthalten, aber auch Fotos von Menschen, die zur Fahndung ausgeschrieben oder die einer erkennungsdienstlichen Behandlung unterzogen wurden." (Beitrag 4)*

Dabei wird nicht weiter erläutert, was eine erkennungsdienstliche Behandlung bedeutet und unter welchen Voraussetzungen diese erfolgen darf. Andere Artikel sprechen etwa von einer

> *„Straftäter-Datenbank des Bundeskriminalamtes (BKA)" (Beitrag 35)*

oder einer *„deutschlandweite[n] Polizei-Datenbank[, die] […] mittlerweile mit mehr als 5,8 Millionen Aufnahmen von etwa 3,6 Millionen erfassten Straftätern oder Beschuldigten gefüllt [ist]." (Beitrag 25)*

Besonders auffallend ist, dass keiner der Beiträge davon berichtet, dass auch die Bilder aller Asylsuchenden durchleuchtet werden. Auch bleibt unerwähnt, dass mit zur Gefahrenabwehr angelegten Datenbanken abgeglichen wird; darin können insbesondere auch Personen enthalten sein, die nicht Beschuldigte in einem Ermittlungsverfahren waren.

cc) Bedenken mit Blick auf informationelle Selbstbestimmung

Im Zusammenhang mit dem Einsatzszenario der Identifizierung unbekannter Verdächtiger erwähnen die Beiträge nur selten Bedenken mit Blick auf die Privatheit oder informationelle Selbstbestimmung. Von der Gefahr einer Überwachung wird zwar allgemein im Zusammenhang mit Gesichts-

erkennung gesprochen, speziell beim Anwendungsszenario der Identitätsermittlung ist aber nur vereinzelt von *„Überwachung“ (Beitrag 10, Beitrag 31)* die Rede. Ein Beitrag verweist in diesem Zusammenhang zumindest darauf, dass die Technologie daher für die Strafverfolgungsbehörden so attraktiv sei:

> *„Jeden Verdächtigen sofort erkennen und auf Schritt und Tritt verfolgen: Für Polizeibehörden auf der ganzen Welt ist Gesichtserkennung hochattraktiv.“ (Beitrag 31)*

Einige Beiträge erwähnen, dass die Anzahl der gespeicherten und durchsuchbaren Fotos angestiegen sei. Exemplarisch ist die folgende Passage:

> *„In der zentralen Polizeidatenbank speichern die teilnehmenden Behörden zeitlich begrenzt Informationen zu Inhaftierten, sowie zu Menschen, die zur Fahndung ausgeschrieben oder einer erkennungsdienstlichen Behandlung unterzogen wurden. Zu einer Person können dort mehrere Bilder gespeichert werden. Die Zahl der Gesichtsbilder ist in dreieinhalb Jahren um rund eine Million Fotos gestiegen. Im Mai 2016 waren erst rund 4,86 Millionen Lichtbilder von 3,34 Millionen Menschen eingestellt.*
> *‚Das BKA muss diesen Zuwachs erklären‘, forderte Hunko. Der zunehmende Einsatz von Software zur Verarbeitung von Massendaten habe offensichtlich zu einem regelrechten ‚Datenhunger‘ geführt.“ (Beitrag 4)*

dd) Überprüfung der Treffer durch Menschen

Die menschliche Überprüfung der per Gesichtserkennung generierten Treffer wird als sinnvolle Kontrolle dargestellt:

> *„Gesichtsexperten gleichen die Bilder dann noch einmal ab, um auf Nummer sicher zu gehen.“ (Beitrag 35)*

> *„‚Für die Polizei ist es kein Problem, wenn sie zehn Verdächtige angezeigt bekommt statt nur einer Person‘, sagt [Interviewpartner und Professor für Medieninformatik] Florian Gallwitz. Die Beamten hätten dann trotzdem vergleichsweise schnell einen Kreis an Verdächtigen und könnten von dort aus weiter ermitteln.“ (Beitrag 35)*

Dass den Menschen bei der Auswahl des richtigen Treffers ebenfalls Fehler unterlaufen können, wie es die oben erwähnte Forschung zeigt,[1048] wird nicht erwähnt.

3. Darstellung der Fehleranfälligkeit der Technologie

a) Hohe Fehlerquoten

Beinahe alle Beiträge, die sich zur Leistungsfähigkeit von Gesichtserkennungssystemen äußern, stellen die Technologie als fehleranfällig dar. Nur ein Beitrag sprach ohne nähere Erläuterung oder Nennung einer Quelle von einer *„Trefferquote von über 99 Prozent" (Beitrag 4)*. Die übrigen Beiträge bezeichnen die Fehleranfälligkeit als *„hoch" (Beitrag 23)*, Gesichtserkennung sei *„für die Tonne" (Beitrag 15)*. Um dies zu verdeutlichen, verweisen einige Artikel auf vergangene Tests:

> *„Tests mit Gesichtserkennung in London und New York zeigten, dass entsprechende Systeme grundsätzlich fehleranfällig sind. Sie schlugen in 81 Prozent der Fälle fehl oder erkannten niemanden. Ähnliche Resultate ergab auch eine Testreihe der Bundespolizei am Berliner Südkreuz." (Beitrag 11)*

Obwohl sich der Beitrag mit dem Einsatz automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger und dem Risiko von Fehlidentifizierungen befasst, werden hier Testergebnisse für ein anderes Szenario – Echtzeit-Gesichtserkennung im öffentlichen Raum – herangezogen, ohne dies kenntlich zu machen oder zu erläutern. Tatsächlich sind die erwähnten hohen Fehlerquoten beim Einsatz zur Identifizierung nicht zu erwarten. Bei der Gesichtserkennung im öffentlichen Raum ist beinahe jede versuchte Erkennung eine Herausforderung für die Technologie, da die aufgezeichneten Personen nicht in Richtung der Kamera blicken und häufig ungünstige Lichtverhältnisse und ein großer Abstand zur Kamera bestehen. Die Suchbilder bei der Identifizierung unbekannter Verdächtiger können hingegen regelmäßig eine gute Qualität aufweisen, etwa wenn der Verdächtige anhand seines Profilfotos, eines Fotos auf einer Nachtclub-

1048 Kapitel III. B. II. 2. a).

Webseite oder einer Bildaufnahme aus nächster Nähe durch einen Zeugen identifiziert werden soll.[1049]

b) Verweis auf öffentlichkeitswirksamen „Test" durch die ACLU

Besonders häufig wird in Beiträgen auf einen öffentlichkeitswirksamen „Test" durch die American Civil Liberties Union (ACLU), eine US-amerikanische NGO, verwiesen.[1050] Das Gesichtserkennungssystem „Rekognition" von Amazon hatte fälschlicherweise eine Übereinstimmung von 28 Mitgliedern des US-Kongresses mit Fahndungsfotos festgestellt. Exemplarisch sind folgende Textpassagen:

> *„Ein Experiment der Organisation American Civil Liberties Union aus dem Jahr 2018 zeigt, dass Amazons Programm Rekognition 28 Kongressmitglieder fälschlicherweise mit Personen identifizierte, die wegen eines Verbrechens festgenommen wurden." (Beitrag 12)*

> *„Auch Amazons Rekognition-Technologie hat sich in der Vergangenheit als fehleranfällig gezeigt: In einem Versuch der American Civil Liberties Union von Nordkalifornien hat Rekognition 28 Kongressmitglieder fälschlicherweise als auf Fahndungsbildern gesuchte Personen ausgewiesen." (Beitrag 7)*

> *„Um Druck auf die Abgeordneten zu machen, hatte die Bürgerrechtsorganisation ACLU schon 2018 zu einem cleveren Trick gegriffen. Sie ließ die 535 Abgeordneten des US-Parlaments mit einer Datenbank von 25.000 Fahndungsbildern abgleichen – und fand unter den hochrangigen Politikern 28 Treffer. Der Großteil der zu Unrecht als Verbrecher erkannten Abgeordneten war dunkelhäutig." (Beitrag 31)*

Unerwähnt bleibt in diesem Zusammenhang jedoch in allen Beiträgen, dass die ACLU die Standardeinstellung des Systems für Übereinstimmungen – einen Schwellenwert (Confidence threshold) von 80 % – verwendet hatte. Daher wurde jedes Gesicht mit einem Ähnlichkeitswert von 80 % oder mehr als Treffer gewertet. Für die Verwendung von Gesichtserkennung im privaten Alltag ist ein Ähnlichkeitswert von lediglich 80 % meist ausreichend (und sogar sinnvoll), etwa um Fotos auf dem Smartphone nach einer

1049 Siehe die Beispiele in Kapitel I. G. I. 3.
1050 *Snow*, ACLU News & Commentary v. 26.7.2018, https://perma.cc/D847-DUG5.

bestimmten Person zu filtern; falsch zugeordnete Personen können dann einfach manuell aussortiert werden.[1051] Dagegen wird für die Anwendung durch Strafverfolgungsbehörden ein deutlich höherer Ähnlichkeitswert von 95 % empfohlen, um falsche Übereinstimmungen zu vermeiden.[1052] Zwar könnten die Strafverfolgungsbehörden – entgegen möglichen internen Vorgaben – einen niedrigeren Schwellenwert einstellen, um Treffer zu erzielen. Aber das Problem läge dann nicht in der Technologie, sondern in der menschlichen Interaktion mit der Technologie – was ein eigenständiges Problem ist und als solches behandelt werden sollte.

c) Gesichtserkennung als rassistische Technologie

Viele Beiträge bringen Gesichtserkennung mit Rassismus in Verbindung. In einigen Artikel ist mit Blick auf die Technologie etwa von *„Rassismus per Software" (Beitrag 12)* oder *„Rassismus in Algorithmen" (Beitrag 15)* die Rede. In den meisten dieser Beiträge wird durch die Formulierung nahegelegt, dass alle Gesichtserkennungssysteme hiervon betroffen seien.

> *„Erkennungsysteme [sic!] besitzen eine besonders hohe Fehlerquote bei dunkelhäutigen Gesichtern." (Beitrag 9)*

> *„Gesichtserkennung liegt bei dunkelhäutigen Personen deutlich häufiger falsch." (Beitrag 31)*

Zwar verweisen die Artikel darauf, dass die Ursache vor allem in unausgewogenen Trainingsdatensätzen liegt. Beispielhaft ist die folgende Passage:

> *„Die Programme trainieren ihre Fähigkeiten, indem sie immer wieder dieselben gigantischen Datensätze miteinander vergleichen. Sind in den Bild-Datenbanken soziale Gruppen unterrepräsentiert, etwa weil die Entwickler ihre eigenen Fotos nutzen, zeichnet sich das auch in der Erkennungsquote ab." (Beitrag 31)*

Dennoch machen nur wenige Beiträge deutlich, dass nicht alle Gesichtserkennungssysteme hiervon betroffen sind, ein Beitrag formuliert zumindest,

1051 So bereits Kapitel I. E. IV. 3. Ähnlich auch *Schindler*, Biometrische Videoüberwachung, 2021, 173.

1052 So auch eine Amazon-Sprecherin zur New York Times, siehe *Singer*, The New York Times v. 26.7.2018, https://perma.cc/4BP3-HHV8.

dass Gesichtserkennungssysteme „*im Allgemeinen*“ (Beitrag 33) bei People of Color deutlich schlechter abschnitten.

4. Berichte über Festnahmen Unschuldiger in den USA

Rund ein Drittel der analysierten Beiträge berichten von Fällen, in denen Unschuldige in den USA nach einem falschen Gesichtserkennungstreffer festgenommen wurden. Auffallend ist, dass die meisten die Verantwortung bei der Technologie sehen. Nur wenige Beiträge deuten zumindest an, dass es so große optische Unterschiede zwischen dem Täter und dem festgenommenen Verdächtigen gab, dass dies den Polizisten hätte auffallen müssen:

> „*Schon in der ersten Befragung wurde klar, dass Williams nicht der gefilmte Übeltäter war. Nach Ansicht der NGO American Civil Liberties Union (ACLU) hätte es für diese Erkenntnis keiner Festnahme, sondern lediglich eines menschlichen Blicks auf die Bilder bedurft, und reichte in Williams Namen Beschwerde gegen das Detroit Police Department ein.*“ *(Beitrag 15)*

Lediglich ein Beitrag geht auf die Problematik ein, dass Gesichtserkennung zu mehr Fehlidentifizierungen durch Menschen beitragen könnte. Zitiert wird eine US-amerikanische Strafverteidigerin mit folgendem Statement:

> „*Stellen Sie sich nun vor, Sie stehen als Zeuge vor Gericht und grübeln, ob es tatsächlich diese Person war, die sie gesehen haben. Da fühlt es sich doch super an, wenn ihnen ein Polizist gesagt hat: ‚Wir haben den Kerl längst identifiziert mit unserer Technologie. Wir brauchen nur noch Ihre Bestätigung.‘ Wie groß ist da die Versuchung zu denken: ‚Es hängt gar nicht von mir ab. Die Technologie hat die Entscheidung getroffen und ich kann ihr vertrauen.‘*“ *(Beitrag 5)*

In den anderen Beiträgen kommt die menschliche Verantwortung für Fehlidentifizierung nicht zum Ausdruck. Dies zeigt sich bereits in den Überschriften, die so formuliert sind, dass die Gesichtserkennung verantwortlich gemacht wird:

> „*Gesichtserkennung: Zehn Tage im Knast wegen KI-Fail*“ *(Beitrag 11)*

> „*Gesichtserkennung: Algorithmus führt zur Verhaftung eines Unschuldigen*“ *(Beitrag 16)*

„Wegen fehlerhafter Gesichtserkennung nimmt Polizei hochschwangere Frau fest" (Beitrag 23)

„Gesichtserkennung: Fehler brachte US-Bürger unschuldig ins Gefängnis" (Beitrag 9)

„USA: Fehler bei Gesichtserkennungs-Software – Mann unschuldig im Gefängnis" (Beitrag 26)

„Software zur Gesichtserkennung versagt – Polizei nimmt hochschwangere Frau fest" (Beitrag 17)

Auch in den Texten wird das Geschehen so dargestellt, dass die Ursache vor allem in der Gesichtserkennungstechnologie liegt. Porcha Woodruff sei zu Unrecht festgenommen worden, *„[w]eil eine Polizei-KI sie für die Täterin hielt." (Beitrag 3)*. In einem Beitrag ist etwa von einem *„KI-Fail"* und einer *„KI-Panne"* die Rede *(Beitrag 11)*. Die Festnahmen würden ein Versagen der Software zeigen:

„Nun musste ein Mann unrechtmäßig hinter Gitter, weil die Gesichtserkennung der Software versagte.
[…]
Der Vorfall zeigt erneut, was passieren kann, wenn Gesichtserkennung fehlschlägt. Der US-Amerikaner Robert Julian-Borchak Williams wurde im Sommer ebenfalls wegen einer KI-Panne unrechtmäßig verhaftet." (Beitrag 11)
„In den USA ist es zu mehreren falschen Verhaftungen gekommen, für die Gesichtserkennung verantwortlich zeichnet. […] Laut einem Bericht der New York Times hat Gesichtserkennung in den USA in drei Fällen zu falschen Verhaftungen geführt. Nijeer Parks die dritte bekannte Person, die aufgrund einer schlechten Gesichtserkennung fälschlicherweise für ein Verbrechen verhaftet wurde, das sie nicht begangen hat." (Beitrag 16)

Auch Beiträge, die erwähnen, dass ein auffälliger Unterschied zwischen Täter und Festgenommenem bestand, deuten eine mögliche Verantwortung der Polizisten nur an. Ein Beitrag beschreibt die Festnahme beispielsweise zunächst als Fehler der Technologie:

„Auf Grund eines Fehlers bei einer Gesichtserkennungssoftware wurde in den USA ein Mann unschuldig für neun Tage eingesperrt. […] Das Obskure an der Geschichte ist, dass der Mann unschuldig war und der Software ein Fehler unterlaufen ist." (Beitrag 26)

Erst zum Ende des Beitrags wird in einem Satz angedeutet, dass die Polizisten ihn trotz optischer Unterschiede festnahmen.

> *„Hier stimmten weder Gewicht noch Größe mit der Täterbeschreibung überein. Und dennoch beschuldigten die Behörden den Mann." (Beitrag 26)*

Ein Beitrag wies sogar, im Gegenteil, ausdrücklich die Verantwortung von den Menschen weg und der Technologie zu:

> *„Der Fehler lag aber nicht im Rassismus eines Menschen. Die Polizisten hatten nur ihren Job gemacht. Es war eine Maschine, die Julian-Borchak verwechselt hatte." (Beitrag 34)*

IV. Diskussion und Schlussfolgerungen

1. Unklarheit über Einsatz in Deutschland

Die Medienanalyse zeigt, dass verschiedene Beiträge ein sehr unterschiedliches Bild von Gesichtserkennung zeichnen und häufig ein unvollständiges oder unzutreffendes Bild vermitteln. Zwischen den verschiedenen Einsatzszenarien von automatisierter Gesichtserkennung wird meist nicht differenziert. Die Tatsache, dass auch in Deutschland Strafverfolgungsbehörden die Technologie bereits zur Identifizierung unbekannter Verdächtiger einsetzen, wird in vielen Beiträgen zu diesem Thema nicht erwähnt, was darauf hindeutet, dass dies nicht bekannt ist. Welche Datenbanken zum Abgleich herangezogen werden, wird sehr unterschiedlich beschrieben, kein Beitrag zeichnete hier ein korrektes und vollständiges Bild. Diese Befunde deuten darauf hin, dass in den Medien eine große Unklarheit besteht, wie Gesichtserkennung derzeit in Deutschland zur Strafverfolgung eingesetzt wird. Dies legt zumindest nahe, dass auch in der Bevölkerung hier wenig Klarheit herrscht.

Eine solche Erkenntnis überrascht nicht, da derzeit keine Berichtspflichten, etwa für die Öffentlichkeit, über die Verwendung automatisierter Gesichtserkennung bestehen. Die Informationen zum Einsatz in Deutschland stammen aus Kleinen Anfragen von Abgeordneten oder aus Interviews mit Behördenvertretern. Es überrascht nicht, dass daraus kein fundiertes Verständnis der Technologie und ihrer Probleme erwachsen kann.

Der Einsatz automatisierter Gesichtserkennung in der Strafverfolgung ist aber eine so grundlegende, die Gesellschaft berührende Frage, dass die

Öffentlichkeit zumindest die Möglichkeit haben muss, sich hierüber zu informieren und eine durchdachte Meinung zu bilden. Dies ist gegenwärtig nicht möglich. Bei der Regulierung der Verwendung von Gesichtserkennung zur Identifizierung unbekannter Verdächtiger sollte daher nicht nur aus verfassungsrechtlichen Gründen eine Berichtspflicht geregelt werden, sondern auch, um eine demokratische Debatte über eine wirkmächtige Technologie zu ermöglichen, die in vielerlei Hinsicht die Gesellschaft tangiert. Dies gilt umso mehr, als die Medienanalyse einen Eindruck davon vermittelt, wie intensiv das Thema automatisierte Gesichtserkennung in der Strafverfolgung diskutiert wird.

2. Bedenken

Die Untersuchung gibt zudem Hinweise darauf, welche Bedenken beim Einsatz automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger im Vordergrund stehen. Dabei ist zunächst zu beachten, dass, wie oben angesprochen, viele Beiträge nicht näher zwischen verschiedenen Einsatzszenarien differenzieren. Automatisierte Gesichtserkennung dürfte daher teilweise „einheitlich" als eine problematische Technologie wahrgenommen werden. Die in Kapitel II. herausgearbeitete Anforderung, dass eine Rechtsgrundlage durch Benennung des Maßnahmezwecks klar zwischen verschiedenen Szenarien differenzieren muss, wird hierdurch bekräftigt.

Speziell mit Blick auf die Einsatzvariante der Identifizierung unbekannter Verdächtiger fällt auf, dass selten Bedenken hinsichtlich der Privatheit und der informationellen Selbstbestimmung geäußert wurden. Dies mag damit zusammenhängen, dass in den Medien das unzutreffende Bild vermittelt wird, nur „Straftäter" seien in den durchsuchten Datenbanken gespeichert. Jedenfalls aber sollte der Umstand, dass dies die Medien nicht näher problematisieren (und daher von der Politik auch keine Änderungen eingefordert werden), für die Rechtswissenschaft ein Appell sein, besonders wachsam zu bleiben, Inhalt und Ausmaß der Datenbanken kritisch zu hinterfragen und gegebenenfalls nachdrücklich auf die Kriminalpolitik einzuwirken.

Große Bedenken im Zusammenhang mit der Verwendung von Gesichtserkennung zur Identitätsermittlung scheinen aber hinsichtlich der Fehleranfälligkeit der Technologie zu bestehen. Zwar wird in den hier analysier-

ten Beiträgen fast durchweg ein verzerrtes Bild von der Fehleranfälligkeit der Technologie vermittelt. Da der überwiegende Teil der Bevölkerung wohl kaum auf wissenschaftliche Untersuchungen (etwa des NIST) oder sonstige Fachliteratur zurückgreifen wird, dürfte dieses Bild auch in den Köpfen der Menschen vorherrschen. Darüber hinaus wird mehrheitlich der Eindruck vermittelt, dass alle Gesichtserkennungssysteme rassistisch verzerrt seien, also höhere Fehlerraten für einige ethnischen Gruppen aufweisen. Dies trifft zwar in dieser Pauschalität nicht zu,[1053] insbesondere sehr leistungsfähige, wenig fehleranfällige Algorithmen weisen oft auch vergleichbare (geringe) Fehlerraten für verschiedene Bevölkerungsgruppen auf. Aber auch dieser medial vermittelte Eindruck einer „rassistischen Technologie" dürfte vorerst in der Bevölkerung bestehen.

Um diesen Bedenken zu begegnen, sollte sichergestellt werden, dass die deutschen Strafverfolgungsbehörden nur Gesichtserkennungssysteme verwenden, die nach dem aktuellen Stand der Technik ein Höchstmaß an Genauigkeit aufweisen, unabhängig evaluiert und durch eine (noch einzurichtende Stelle) zertifiziert sind;[1054] die Ergebnisse der externen Evaluation sollten öffentlich einsehbar sein. Vor allem muss offengelegt werden, ob und wie stark sich Fehlerraten für verschiedene Bevölkerungsgruppen unterscheiden. Dies bekräftigt erneut den oben gemachten Vorschlag[1055], dass eine Kontrolle des Einsatzes automatisierter Gesichtserkennung nicht nur durch einen Datenschutzbeauftragten erfolgen sollte, sondern dass eine umfassendere Kontrolle und Evaluation erforderlich sind. Diese könnte beispielsweise auch untersuchen, ob und in welchen Fällen es im Zusammenhang mit Gesichtserkennung zu Ermittlungen gegen Unbeteiligte kommt und ob dies bei bestimmten Personengruppen häufiger vorkommt.[1056]

3. Sekundärer Automation bias in den Medien

Die Medienanalyse verdeutlicht, dass die Fehleranfälligkeit der Technologie und ihre Verantwortung für Ermittlungen gegen Unschuldige überhöht dargestellt werden. Der Faktor Mensch wird in diesem Zusammenhang kaum erwähnt. Insbesondere die oben herausgearbeitete Problematik, dass

1053 Hierzu Kapitel I. E. IV. 5.
1054 Zur Ausgestaltung Kapitel IV. A. II.
1055 Kapitel II. A. I. 3. c) cc.)
1056 Zur Ausgestaltung Kapitel IV. C. II.

auch Menschen regelmäßig Fehler bei der Gesichtserkennung unterlaufen und dass ein Automation bias dies noch verstärken wird, sehen die analysierten Medienbeiträge nicht. Die menschliche Verantwortung für die Festnahmen Unschuldiger wird daher überwiegend übersehen.

Dies deutet auf ein weiteres, bislang noch nicht benanntes Phänomen hin: Im ersten Schritt unterliegt ein Mensch, der mit einer Maschine interagiert, einem Automation bias; er verlässt sich auf die Technologie und übersieht seine eigene Verantwortung. In einem zweiten Schritt übersehen dies nun aber wiederum die Medien und schreiben die Verantwortung allein der Technologie zu; sie unterliegen einem *sekundären* Automation bias. Auf ein solches Phänomen kann die hier vorgenommene Medienanalyse nur hindeuten; es erscheint jedoch lohnenswert, dieses in Zukunft näher empirisch zu untersuchen.

Jedenfalls sollte der Gesetzgeber bei einer Regulierung der automatisierten Gesichtserkennung einer solchen verzerrten Wahrnehmung nicht unterliegen. Die im obigen Abschnitt (Kapitel II. B. II.) herausgearbeiteten, vor allem *menschlichen* Ursachen für Fehler im Zusammenhang mit Gesichtserkennung und Maßnahmen gegen Unschuldige sollten bei der Ausgestaltung einer Rechtsgrundlage und weiteren Vorgaben berücksichtigt werden.

D. Fazit zu Kapitel III. Folgen und mediale Darstellung des Einsatzes automatisierter Gesichtserkennung – kriminologische Betrachtung

Der Einsatz automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger birgt das Potenzial, unbeabsichtigte problematische Folgen mit sich zu bringen. Die Technologie wird sich auf die ohnehin bereits bestehende Selektivität der Strafverfolgung auswirken. Bagatellkriminalität könnte in Zukunft deutlich leichter und daher häufiger verfolgt werden. Zudem droht eine noch stärkere Verschiebung der Strafverfolgung hin zu Menschen, die bereits mit der Polizei in Kontakt kamen oder die – wie Asylsuchende – aus anderen Gründen in der durchsuchbaren Datenbank gespeichert sind. Eine solche Auswirkung auf den strafrechtlichen Selektionsprozess sollte nicht unbemerkt vor sich gehen, sondern kriminologisch untersucht und kriminalpolitisch hinterfragt werden.

Automatisierte Gesichtserkennung kann auch Folgen für Unbeteiligte haben, insbesondere dazu führen, dass noch häufiger Ermittlungsverfahren gegen Unschuldige geführt werden und dass der Fehler nicht oder erst

spät erkannt wird. Eine nähere Betrachtung der Fälle von Festnahmen Unschuldiger in den USA nach falschem Gesichtserkennungstreffer zeigt, dass hierfür nicht nur Fehler der Technologie, sondern vor allem Fehler von Menschen ursächlich sind. Dieses Risiko gilt es bei der Regulierung von Gesichtserkennung zu adressieren und einzuhegen (zur konkreten Umsetzung siehe Kapitel IV.).

Die Medienanalyse hat gezeigt, dass offenbar noch eine große Unklarheit besteht, ob und wie deutsche Strafverfolgungsbehörden automatisierte Gesichtserkennung einsetzen. Es wird zudem ein verzerrtes Bild speziell des Einsatzes zur Identifizierung unbekannter Verdächtiger vermittelt. Eine informierte öffentliche Debatte über automatisierte Gesichtserkennung ist daher schwer möglich. Mit Blick auf die Bedenken zeigt sich, dass die Fehleranfälligkeit der Technologie und der Vorwurf rassistisch verzerrter Algorithmen im Vordergrund stehen. Aus verfassungsrechtlichen Gründen ist ohnehin geboten, eine Technologie auf dem aktuellen Stand der Technik einzusetzen; darüber hinaus sollte eine Evaluierung der eingesetzten Systeme nicht zuletzt aufgrund der Bedenken hinsichtlich der Fehleranfälligkeit angeordnet werden. Die Medienanalyse macht zudem deutlich, dass Fehler beim Einsatz automatisierter Gesichtserkennung tendenziell der Technologie zugeschrieben, die menschliche Verantwortung und ein möglicher Automation bias hingegen regelmäßig übersehen werden; dieses Phänomen lässt sich unter dem Begriff *sekundärer* Automation bias zusammenfassen. Der Gesetzgeber sollte einer solchen Verzerrung bei einer Regulierung automatisierter Gesichtserkennung nicht unterliegen. Eine Rechtsgrundlage muss Regelungen treffen, um menschliche Fehler bei der Interaktion mit Gesichtserkennungssystemen so weit wie möglich zu verhindern.

Kapitel IV. Empfehlungen für eine Regulierung

In diesem Kapitel soll aus den vorangegangenen Erkenntnissen ein konkreter Vorschlag für eine Regulierung des Einsatzes automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger erarbeitet werden. Dieser Vorschlag und die Empfehlungen erheben nicht den Anspruch, vollumfänglich zu sein, sondern sollen den Ausgangspunkt für eine weitere Diskussion in der Rechtswissenschaft und Kriminologie bilden. Besonders wertvoll wäre, hierzu in Zukunft auch in Austausch mit anderen Disziplinen wie der Informatik und der Soziologie zu treten. Insbesondere sollten diese Vorschläge lediglich als Mindestvorgaben verstanden werden; die Frage, inwieweit der Einsatz automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger zugelassen werden soll, bedarf eines rechtspolitischen Diskurses der Öffentlichkeit.

Im Folgenden wird zunächst auf die technischen Anforderungen an Gesichtserkennungssysteme eingegangen (A.), dann werden die Vorgaben für eine Rechtsgrundlage und ein Formulierungsvorschlag erarbeitet (B.) und schließlich weitere Empfehlungen, insbesondere zu Evaluation, Kontrolle und Berichtspflichten, vorgestellt (C.).

A. Technische Anforderungen an die verwendeten Gesichtserkennungssysteme

I. Genauigkeit und Freiheit von demografischen Verzerrungen

Die verwendeten Gesichtserkennungssysteme müssen dem jeweils aktuellen Stand der Technik entsprechen und daran gemessen ein Höchstmaß an Genauigkeit erfüllen.[1057] Näher ausformulierte Vorgaben, etwa zu den Fehlerraten, sind wegen des schnellen technologischen Fortschritts nicht ratsam. Festgelegt werden sollte zudem, dass die Systeme von einer unab-

1057 Vgl. auch *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, 2023, 506, 772 zu einer ähnlichen Formulierung für Regelungen zum Einsatz von statistischen und selbstlernenden Data Mining-Methoden im Strafverfahren.

hängigen Stelle wie dem NIST[1058], nicht etwa nur von dem Anbieter selbst, evaluiert sein müssen. Zwar ist tendenziell bei den genauesten Gesichtserkennungssystemen zu erwarten, dass sie auch vergleichbare Fehlerraten für unterschiedliche Bevölkerungsgruppen aufweisen;[1059] auf solche Erfahrungswerte sollte beim Einsatz von Gesichtserkennung in einem sensiblen Bereich wie der Strafverfolgung aber nicht abgestellt werden. Stattdessen sollten die eingesetzten Gesichtserkennungssysteme vor ihrem Einsatz von einer unabhängigen Stelle wie beispielsweise dem NIST zusätzlich auch auf demografische Verzerrungen hin untersucht worden sein. Auch wenn die Fehlerraten für verschiedene Bevölkerungsgruppen nicht exakt gleich ausfallen werden, sollten sie sich jedoch in einem vergleichbaren Rahmen bewegen.

II. Einrichtung einer zentralen Zertifizierungsstelle

Um sicherzustellen, dass diese Anforderungen erfüllt sind, ist eine zentrale Zertifizierungsstelle für in der Strafverfolgung verwendete Gesichtserkennungssysteme einzurichten. Diese testet die Systeme nicht selbst,[1060] sondern prüft anhand der Ergebnisse der externen Evaluation, ob das System dem aktuellen Stand der Technik entspricht. Hierüber wird ein Zertifikat ausgestellt. Die Rechtsgrundlage für den Einsatz automatisierter Gesichtserkennung sollte dann festlegen, dass nur von dieser Stelle zertifizierte Gesichtserkennungssysteme eingesetzt werden dürfen. Zudem sollte die Exekutive ermächtigt werden, durch Rechtsverordnung eine solche Stelle zu errichten und das nähere Verfahren (z. B. Dauer der Gültigkeit der Zertifikate) zu regeln.[1061] Ein solcher Regulierungsansatz würde gewährleisten, dass – anders als gegenwärtig der Fall – jede Polizeibehörde, die ein Gesichtserkennungssystem anschafft, dieses zunächst unabhängig evaluie-

1058 Zum NIST Kapitel I. E. IV. 4.

1059 Kapitel I. E. IV. 5.

1060 Hierfür wäre ein großer Ressourcenaufwand (insbesondere eine Testdatenbank und Fachkräfte) nötig, der angesichts der bereits bestehenden verlässlichen und renommierten unabhängigen Bewertungsstellen wie dem NIST nicht sinnvoll erscheint.

1061 Vgl. auch den Vorschlag von *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, 2023, 772 für die Einrichtung von Stellen zur Zertifizierung von Blackbox-Programmen, die zum Data Mining eingesetzt werden.

ren lassen[1062] und dann eine Zertifizierung beantragen muss. So kommen nur Systeme zur Anwendung, die dem Stand der Technik entsprechen. Dies kann angesichts der Bedenken in der Bevölkerung hinsichtlich Fehleranfälligkeit und Diskriminierung durch Gesichtserkennungssysteme[1063] auch dazu beitragen, das Vertrauen in die polizeiliche Arbeit mit neuen Strafverfolgungstechnologien zu erhöhen.

Unter Umständen könnte sich eine solche zentrale Zertifizierungsstelle in Zukunft durch das Konformitätsbewertungsverfahren[1064] nach Art. 43 KI-VO für Hochrisiko-KI-Systeme (also auch für biometrische Fernidentifizierungssysteme wie automatisierte Gesichtserkennung) erübrigen. Dann müsste dieses geeignet sein, sicherzustellen, dass nur Gesichtserkennungssysteme zur Anwendung kommen, die dem aktuellen Stand der Technik entsprechen und daran gemessen ein Höchstmaß an Genauigkeit erfüllen. Derzeit ist dies aber nicht gesichert, denn Art. 15 Abs. 1 KI-VO fordert lediglich ein „angemessenes" Maß an Genauigkeit. Dieser Maßstab soll zukünftig durch Normierungsinstitutionen näher konkretisiert werden. Dies ist nicht unkritisch zu sehen, denn damit gehen regelmäßig auch Wertentscheidungen mit einher.[1065] Gerade für den besonders sensiblen Bereich der Strafverfolgung sollten solche Wertentscheidungen wohlüberlegt, mit äußerster Sorgfalt und unter Berücksichtigung der Konsequenzen für die Betroffenen getroffen werden. Derzeit ist noch nicht abzusehen, ob dies mit den Vorgaben der KI-Verordnung gewährleistet werden kann. Auch wenn der hier unterbreitete Vorschlag einer nationalen Zertifizierungsstelle für Gesichtserkennungssysteme eine weitere Vorgabe für den Einsatz von Gesichtserkennungstechnologie und damit weitere bürokratische Hürden schafft: Solange nicht sichergestellt ist, dass die KI-Verordnung so ausgelegt und konkretisiert wird, dass nur Systeme zur Anwendung kommen, die dem Stand der Technik entsprechen, sollte dies durch eine nationale Zertifizierungsstelle abgesichert werden.[1066]

1062 Oder die Polizei müsste bereits evaluierte Systeme erwerben.

1063 *Kostka/Steinacker/Meckel*, Public Understanding of Science 2021, 671, 683 f.; zur Darstellung von Gesichtserkennung als „rassistische Technologie" Kapitel III. C. III. 2. b) cc) und Kapitel III. C. IV. 2.

1064 Hierzu Kapitel II. B. I. 1. b) aa).

1065 Kritisch auch *Martini*, in: Martini/Wendehorst, KI-VO, Art. 15 Rn. 37; vgl. auch *Guijarro Santos*, ZfDR 2023, 23, 33 f.

1066 Selbstverständlich ließe sich einwenden: Wird dieser Zertifizierungsstelle damit nicht ebenfalls eine Wertentscheidung überlassen? Das ist zutreffend, allerdings wird dieser (notwendige) Umstand durch zwei Faktoren abgemildert: Erstens wird

B. Rechtsgrundlage

I. Vorgaben des Grundsatzes der Bestimmtheit und Normenklarheit

Um dem Grundsatz der Bestimmtheit und Normenklarheit sowie dem Wesentlichkeitsprinzip zu genügen, muss die Rechtsgrundlage zumindest den konkreten Zweck der Maßnahme erkennen lassen, die zum Abgleich zugelassenen Datenbanken beschreiben und begrenzen, das technische Eingriffsinstrument benennen und die Verwendung biometrischer Merkmale offenlegen.

1. Formulierung des Zwecks

Der Zweck der Maßnahme, also die Identifizierung unbekannter Verdächtiger, muss konkret benannt werden.[1067] Eine offene Formulierung wie in § 98c StPO („zur Aufklärung einer Straftat") mag für geringfügige Grundrechtseingriffe ausreichend sein, bei erheblichen Eingriffen wie der Gesichtserkennung muss das Gesetz die Zielrichtung der Maßnahme näher erkennen lassen. Dabei ist eine möglichst genaue Beschreibung wie „zur Identifizierung unbekannter Verdächtiger" zu empfehlen. Zugleich würde dadurch sichergestellt, dass sich die Maßnahmen nur gegen den Beschuldigten, nicht etwa – wie dies bei § 98c StPO möglich ist – gegen Zeugen richten dürfen.

2. Begrenzung der Datenbanken

Der Gesetzgeber muss zudem die zum Abgleich zugelassenen Datenbanken klar benennen und dadurch wirksam begrenzen.[1068] Besonders kritisch

---

in dieser Arbeit vorgeschlagen, dass die Systeme nicht nur ein „angemessenes" Maß, sondern ein Höchstmaß an Genauigkeit aufweisen müssen. Zweitens könnte die in dieser Arbeit ebenfalls vorgeschlagene – siehe unten – noch einzusetzende interdisziplinär besetzte Evaluationskommission von Gesichtserkennungssystemen die Entscheidungen der Zertifizierungsstelle kritisch hinterfragen und so einen Diskurs anstoßen; dessen Ergebnisse könnten dann auch realistisch zeitnah (anders als bei Normierungsinstituten auf EU-Ebene) in Deutschland umgesetzt werden.

1067 Kapitel II. A. I. 3. b) und Kapitel II. C. I. 2. a).

1068 Kapitel II. A. I. 3. b) und Kapitel II. C. I. 2. c).

sollte hinterfragt werden, ob pauschal bei jeder Gesichtserkennungssuche – wie derzeit mit dem BKA-GES praktiziert –[1069] ein Abgleich mit den Lichtbildern aller Asylsuchenden zulässig sein kann. Solche grundlegenden Fragen zur Streubreite der Maßnahme und damit zur Anzahl der Grundrechtseingriffe muss im Rahmen eines demokratischen Prozesses entschieden werden. Bei Erlass der Rechtsgrundlage für eine neue Datenbank muss der Gesetzgeber dann stets auch neu entscheiden, ob diese per Gesichtserkennung durchsucht werden darf, um unbekannte Verdächtige zu identifizieren.

3. Benennung des technischen Eingriffsinstruments

Weiterhin ist in der Rechtsgrundlage das technische Eingriffsinstrument – die automatisierte Gesichtserkennung – eindeutig zu benennen.[1070] Die Vorschrift des Art. 61 Abs. 2 BayPAG, die insbesondere den Einsatz von Gesichtserkennungssoftware erlauben soll,[1071] sieht beispielsweise vor, dass der Abgleich personenbezogener Daten „auch unter Verwendung bildverarbeitender Systeme und durch Auswertung biometrischer Daten erfolgen" kann. Eine solch offene Beschreibung des technischen Eingriffsinstruments erscheint im sensiblen Bereich der Verarbeitung biometrischer Daten zu unbestimmt. Unter die Formulierung würden sich nicht nur Gesichtserkennungssysteme, sondern auch andere biometrische Identifizierungssysteme[1072] und sogar Emotionserkennungssysteme[1073] subsumieren lassen; diese bedürfen jedoch einer anderen verfassungsrechtlichen und kriminalpolitischen Betrachtung sowie anderer Schutzvorkehrungen als die Gesichtserkennung. Eine Rechtsgrundlage für den Einsatz von Gesichtserkennung sollte dieses technische Eingriffsinstrument ausdrücklich benennen. So lässt die Vorschrift die zugelassene Maßnahme für den Rechtsanwender und Betroffene erkennen und begrenzt zugleich das Eingriffsinstrument.

1069 Kapitel I. F. I. 1.
1070 Kapitel II. A. I. 3. b) und Kapitel II. C. I. 2. b).
1071 BayLT-Drs.17/20425, 82 („Gesichtsfelderkennung").
1072 Zu anderen biometrischen Erkennungssystemen siehe Kapitel I. C. I. 1.
1073 Nach Art. 3 Nr. 39 KI-VO ist ein Emotionserkennungssystem ein „KI-System, das dem Zweck dient, Emotionen oder Absichten natürlicher Personen auf der Grundlage ihrer biometrischen Daten festzustellen oder daraus abzuleiten"; vgl. auch Kapitel I. C. I. 2.

4. Ausdrückliche Nennung der Art biometrischer Merkmale (Gesichtsmerkmale)

Die Rechtsgrundlage muss auch zum Ausdruck bringen, dass nicht nur personenbezogene, sondern gerade biometrische Daten verarbeitet werden. Dies ergibt sich aus dem Verfassungsrecht,[1074] jedenfalls aber aus der JI-Richtlinie[1075]. Den Gesichtsmerkmalen kommt gegenüber anderen biometrischen Merkmalen darüber hinaus eine Sonderstellung zu.[1076] Im Vergleich zu verhaltensbezogenen (dynamischen) Merkmalen wie etwa Stimme, Unterschrift oder Anschlagrhythmus der Tastatur handelt es sich bei Gesichtsmerkmalen um physische biometrische Merkmale: Das Gesicht ist angeboren und weitgehend unveränderlich. Daher können durch Gesichtserkennung gewonnene Informationen eine besondere Persönlichkeitsrelevanz aufweisen. Dem Gesicht kommt auch eine herausgehobene Stellung gegenüber anderen physischen biometrischen Merkmalen wie etwa Fingerabdrücken zu, denn das Gesicht ist selbst aus einer Distanz leicht erkennbar, auf Fotos oder Videos einfach heimlich erfassbar und kann schwerlich versteckt werden, ohne Aufsehen zu erregen. Daher sollte die Rechtsgrundlage nicht nur zu erkennen geben, dass biometrische Merkmale verwendet werden,[1077] sondern die Verarbeitung von Gesichtsmerkmalen benennen. Wenn – wie nach hier vertretener Auffassung – allerdings bereits das technische Eingriffsinstrument (automatisierte Gesichtserkennung) genau benannt werden muss, ist dadurch zugleich auch die Verarbeitung biometrischer Gesichtsmerkmale offengelegt.

II. Verfahrensregelungen

1. Benachrichtigungs-, Kennzeichnungs- und Löschpflichten

Festzulegen ist zudem eine Benachrichtigungspflicht mit Blick auf die Person, gegen die nach einer Gesichtserkennungssuche weiterermittelt wird.[1078] Dabei ist es kriminalpolitisch empfehlenswert, die Vorschrift des

1074 Kapitel II. A. I. 3. b) und Kapitel II. C. I. 2. d).
1075 Kapitel II. B. I. 2. a).
1076 Hierzu Kapitel II. A. I. 2. b) dd).
1077 Wie etwa Art. 61 Abs. 2 BayPAG.
1078 Hierzu Kapitel II. A. I. 3. c) bb). Wie bereits angesprochen, ist eine Benachrichtigung der anderen Personen (Nichttreffer sowie Treffer, die dann aber nicht als

§ 101 StPO, die einheitlich Verfahrensregeln für verdeckte Maßnahmen festlegt, zu erweitern und die neu zu schaffende Rechtsgrundlage dort aufzuführen (zur Benachrichtigungspflicht siehe § 101 Abs. 4 bis 7 StPO).

Auch die Pflicht zur Kennzeichnung personenbezogener Daten (§ 101 Abs. 3 StPO) und Vorgaben für die Löschung der erlangten Daten (§ 101 Abs. 8 StPO) sollten übernommen werden, um die durch den Einsatz von Gesichtserkennung erlangten sensiblen Informationen zu schützen.

2. Richtervorbehalt

Eine Bewilligung durch ein Gericht könnte, wenn nicht bereits aus verfassungsrechtlichen,[1079] so doch zumindest aus kriminalpolitischen Erwägungen vorgeschrieben werden. Zwar ist das Rechtsinstitut des Richtervorbehalts, jedenfalls in seiner gegenwärtigen Ausgestaltung,[1080] zu Recht erheblicher Kritik ausgesetzt. Problematisiert wird insbesondere, dass aufgrund mangelnder Zeit, mangelnder Spezialisierung der Ermittlungsrichter und mangelnder Anreize nur ein geringer Teil der Anträge abgelehnt wird,[1081] und dies, obwohl die Qualität vieler Anträge empirischen Untersuchungen zufolge fragwürdig ist[1082]. Der Richtervorbehalt sei zu einem „Placebo"[1083] verkommen, zu einem „schlichten Feigenblatt ohne nennenswerte eingriffs-

Verdächtige identifiziert wurden) verfassungsrechtlich nicht angezeigt. Sie wäre nicht durchführbar und im Übrigen müssten für eine Benachrichtigung Namen und Adressen dieser Personen anhand der INPOL-Eintragung festgestellt werden; das würde den Grundrechtseingriff noch vertiefen. Siehe erneut zur Vereinbarkeit einer solchen Ausnahme von der Benachrichtigungspflicht für nur unerheblich betroffene Personen mit Art. 13 JI-RL *Schindler*, Biometrische Videoüberwachung, 2021, 717.

1079 Kapitel II. A. I. 3. c) aa)

1080 Dies betont *Voßkuhle*, in: Merten/Papier, Handbuch der Grundrechte, Bd. V, 2013, § 131 Rn. 100.

1081 Überblick über die Schwächen der derzeitigen Ausgestaltung des Richtervorbehalts etwa bei *Voßkuhle*, in: Merten/Papier, Handbuch der Grundrechte, Bd. V, 2013, § 131 Rn. 98.

1082 Vgl. die Nachweise bei *Voßkuhle*, in: Merten/Papier, Handbuch der Grundrechte, Bd. V, 2013, § 131 Rn. 96; vgl. zu rechtstatsächlichen Untersuchungen auch *Brüning*, Der Richtervorbehalt im strafrechtlichen Ermittlungsverfahren, 2005, 195 ff.

1083 *Stadler*, ZRP 2013, 179, 180.

begrenzende Wirkung“[1084]; der Ermittlungsrichter drohe zu einer Art „Urkundsbeamten der Staatsanwaltschaft“ zu denaturieren[1085].

Aber auch wenn eine Reform des Richtervorbehalts[1086] wünschenswert wäre – selbst in seiner gegenwärtigen schwachen Ausgestaltung kann das Rechtsinstitut zumindest einen gewissen Schutz für die von Gesichtserkennung Betroffenen bieten. Dies gilt insbesondere mit Blick auf rechtliche Vorgaben, die nicht der Wertung zugänglich sind und bei denen daher weniger die Gefahr eines „Abnickens“ des Antrags auf Einsatz von Gesichtserkennung besteht. Eine Ermittlungsrichterin könnte etwa sicherstellen, dass die Strafverfolgungsbehörden nur zertifizierte technische Systeme einsetzen oder dass nur qualifizierte Personen den Abgleich und die Identifizierung vornehmen[1087]. Eine Richterin könnte zudem prüfen, ob überhaupt der Verdacht einer Straftat (und nicht etwa nur einer Ordnungswidrigkeit) mit Blick auf die auf dem Suchbild zu sehende Person vorliegt.

3. Subsidiaritätsklausel

Ob ausdrücklich die Subsidiarität[1088] der Identifizierung durch automatisierte Gesichtserkennung geregelt werden sollte, ist hingegen zweifelhaft.[1089] Zwar enthält die Mehrzahl der Vorschriften, die heimliche Ermitt-

1084 *Lilie*, ZStW 111 (1999), 807, 814; vgl. auch *Jahn,* NStZ 2007, 255, 259; *Kutscha*, NVwZ 2003, 1296, 1300.

1085 *Schünemann*, ZStW 114 (2002), 1, 20; vgl. auch *Heghmanns*, GA 2003, 433, 440.

1086 Zusammenfassend zu möglichen Reformen *Voßkuhle*, in: Merten/Papier, Handbuch der Grundrechte, Bd. V, 2013, § 131 Rn. 100; siehe auch bereits *Brüning*, ZIS 2006, 29, 34 f.; *Gusy*, ZRP 2003, 275, 276 ff.; *Helmken*, StV 2003, 193, 196; *Lilie*, ZStW 111 (1999), 807, 816; *Amelung*, Rechtsschutz gegen strafprozessuale Grundrechtseingriffe, 1976, 65.

1087 Zu dieser Vorgabe sogleich unter III. 1.

1088 Zu Subsidiaritätsklauseln auch Kapitel II. C. I. 1. a).

1089 Eine Subsidiaritätsklausel kann neben dem aus Art. 10 JI-RL, § 48 Abs. 1 BDSG folgenden Erfordernis der „unbedingten Erforderlichkeit“ der Datenverarbeitung eine eigenständige Bedeutung haben. Wenn die „unbedingte Erforderlichkeit“ beispielsweise als eine besonders strenge Verhältnismäßigkeitsprüfung verstanden wird (zum Streit Kapitel II. B. I. 2. b)), dann wäre sie zu bejahen, wenn kein *gleich geeignetes* Mittel zur Identifizierung zur Verfügung steht und die Gesichtserkennungsmaßnahme wäre daher – wenn die übrigen Voraussetzungen vorliegen – zulässig. Dagegen könnte in diesem Fall aufgrund einer Subsidiaritätsklausel der Einsatz automatisierter Gesichtserkennung dennoch unzulässig sein, denn eine Subsidiaritätsklausel stellt nicht darauf ab, ob es gleich geeignete Maßnahmen gibt, sondern ob andere Maßnahmen in einem bestimmten Maße *weniger geeignet* sind

lungsmethoden regeln,[1090] eine Subsidiaritätsklausel; damit soll sichergestellt werden, dass diese Maßnahmen nur nachrangig zur Anwendung kommen. Bei der automatisierten Gesichtserkennung ist eine solche abstrakte Nachrangigkeit aber nicht immer sinnvoll. Denn obwohl die automatisierte Gesichtserkennung eine eingriffsintensive und fehleranfällige Maßnahme ist (daher wird in dieser Arbeit eine strenge Regulierung vorgeschlagen), sind gerade ihre *Alternativen*, vor allem die Identifizierung (allein) durch Augenzeugen, unter Umständen sogar noch fehleranfälliger. Selbst wenn ein Zeuge bereits angibt, einen Verdächtigen erkannt zu haben, kann es sinnvoll sein, dennoch eine Gesichtserkennungsrecherche durchzuführen. Das kann etwa der Fall sein, wenn zwischen dem Geschehen und der Identifizierung durch den Zeugen ein großer Zeitabstand liegt. Eine Subsidiaritätsklausel würde aber generell die Nachrangigkeit der automatisierten Gesichtserkennung anordnen, sodass unklar wäre, ob sie in solch einem Fall noch durchgeführt werden dürfte.

4. Verfahren der Identifizierung

Um Ermittlungen gegen Unschuldige so weit wie möglich zu verhindern, sollten besondere Schutzmaßnahmen festgelegt werden. Vor dem Hintergrund der begrenzten menschlichen Fähigkeit zur Gesichtserkennung[1091] sollte die Rechtsgrundlage regeln, dass nur ausgebildete Lichtbildsachverständige und -experten das Gesichtserkennungssystem verwenden und anhand der Kandidatenliste den Verdächtigen identifizieren oder den Verdacht einer Personenidentität feststellen dürfen.[1092] Dies wird, soweit er-

(z. B. „erheblich weniger erfolgversprechend oder wesentlich erschwert" bei § 98a Abs. 1 StPO oder „wesentlich erschwert oder aussichtslos" bei § 100a Abs. 1 StPO).

1090 Eine Ausnahme bilden etwa § 98c StPO und § 163g StPO (automatische Kennzeichenerfassung).

1091 Kapitel III. B. II. 2. a).

1092 Eine besondere Qualifikation der Personen, die eine strafprozessuale Maßnahme vornehmen, regelt beispielsweise auch § 110d S. 2 StPO, wonach bei Beantragung der Maßnahme darzulegen ist, dass die handelnden Polizeibeamten auf den Einsatz umfassend vorbereitet wurden; zur Begründung dieses Erfordernisses BT-Drs. 19/16543, 12. Vgl. auch § 22 Abs. 6 S. 2, § 23 Abs. 4 S. 2 und § 24 Abs. 5 S. 2 TTDSG, die auf Seiten der Anbieter von Telemediendiensten regeln, dass jedes Auskunftsverlangen der Behörden durch eine „Fachkraft" zu prüfen ist (allerdings ohne den Begriff zu definieren).

sichtlich, bei der Verwendung des BKA-GES bereits praktiziert,[1093] ist allerdings nicht gesetzlich geregelt, sodass diese Praxis jederzeit aufgeweicht werden könnte. Auch könnte gegenwärtig eine Polizeibehörde, die selbst ein Gesichtserkennungssystem zur Durchsuchung des lokalen Lichtbildbestands anschafft, einen ungeschulten Polizisten mit dem Abgleich und der Identifizierung betrauen. Dies ist zu verhindern. Auch könnte ausdrücklich geregelt werden, dass die Identifizierung nicht durch eine Person erfolgen darf, die in die Ermittlungstätigkeit dieses Fall involviert ist und daher womöglich voreingenommen ist und vorschnell einen Verdacht annehmen könnte, um einen Ermittlungsansatz zu generieren.[1094] Die Rechtsgrundlage sollte zudem vorsehen, dass im Antrag für den Gerichtserkennungseinsatz darzulegen ist, dass die Personen, die den Abgleich und die Identifizierung vornehmen sollen, hierfür qualifiziert sind. Hier könnte entweder direkt an die Qualifikation als Lichtbildsachverständiger oder -experte[1095] angeknüpft werden („Eine solche Maßnahme dürfen nur Lichtbildsachverständige und Lichtbildexperten treffen") oder – wie in § 110d S. 2 StPO[1096] – eine allgemeinere Formulierung gewählt werden („Eine solche Maßnahme dürfen nur hierfür besonders qualifizierte Personen treffen"). Die handelnden Personen müssen namentlich oder nach ihrer Funktion im Antrag individualisierbar bezeichnet werden.[1097]

Zudem sollte ein echter 4-Augen-Vergleich festgelegt werden. Derzeit wird, soweit ersichtlich, der 4-Augen-Vergleich im Rahmen der Gesichtserkennung so praktiziert, dass ein Experte aus der Kandidatenliste den Verdächtigen auswählt und der zweite Experte lediglich dieses Ergebnis bestätigt oder verwirft. Durch die erste Identifizierung wird aber bereits ein „Anker" geworfen. Stattdessen sollte festgelegt werden, dass die Experten unabhängig voneinander[1098] – also ohne das Ergebnis des anderen zu kennen – dieselbe Person identifizieren bzw. einen Verdacht der Personenidentität feststellen müssen, bevor gegen sie ermittelt werden darf.

Die KI-Verordnung regelt hier keine ausreichenden Schutzmechanismen. Art. 14 Abs. 5 KI-VO schreibt zwar vor, dass zwei natürliche Personen den Treffer bestätigen müssen, allerdings ist diese Vorgabe nicht als Pflicht

1093 Kapitel II. F. I. 2. c)
1094 Kapitel III. B. III.
1095 Zur Ausbildung für diese Qualifikation siehe bereits Kapitel I. F. I. 2. c).
1096 In § 110d StPO S. 2 StPO ist geregelt, dass in dem Antrag darzulegen ist, dass die handelnden Polizeibeamten auf den Einsatz „umfassend vorbereitet wurden".
1097 So mit Blick auf § 110d S. 2 StPO *Rückert/Goger*, MMR 2020, 373, 377.
1098 Vgl. auch die Regelung in § 5 Abs. 1 S. 1 TPG.

der Betreiber ausgestaltet, sondern als (technische) Designvorgabe adressiert an den Anbieter des KI-Systems.[1099] Davon abgesehen ist die Vorgabe, dass diese natürlichen Personen die „notwendige Kompetenz, Ausbildung und Befugnis" haben müssen, wenig konkret und daher jedenfalls für den sensiblen Bereich der Strafverfolgung nicht ausreichend. Auch Art. 26 Abs. 10 Uabs. 3 S. 2 KI-VO bietet keinen genügenden Schutz.[1100]

Wie bereits erwähnt, sollte das Erfordernis der Überprüfung von Treffern einer Kandidatenliste durch Menschen allerdings kritisch hinterfragt werden, wenn in Zukunft deutlich wird, dass die Technologie leistungsfähiger ist als (auch geschulte) Menschen; hierzu sogleich unter IV.

III. Besonderer Schutz der Versammlungsfreiheit

Zusätzliche Voraussetzungen sollte die Rechtsgrundlage für automatisierte Gesichtserkennung festgelegen, wenn es um die Identifizierung von Personen geht, die verdächtigt werden, im Zusammenhang mit einer Versammlung eine Straftat begangen zu haben. Wegen ihres objektiv-rechtlichen Gehalts entfaltet die Versammlungsfreiheit Ausstrahlungswirkungen auf die gesamte Rechtsordnung.[1101] Auch der EGMR hat in seiner Entscheidung zum Einsatz automatisierter Gesichtserkennung Glukhin v. Russland den Versammlungskontext besonders hervorgehoben.[1102] Die Befürchtung, dass beim Verdacht jeder beliebigen, noch so geringfügigen Straftat Videomaterial von einer Versammlung nachträglich per Gesichtserkennung ausgewertet wird, kann Bürgerinnen und Bürger von der Teilnahme abhalten. Der Verdacht einer Straftat kann mitunter schnell begründet sein: Wird bei leichtem Anrempeln eines Polizisten wegen tätlichen Angriffs auf Vollstreckungsbeamte nach § 114 StGB ermittelt, bei einer überspitzten Meinungsäußerung wegen eines Äußerungsdelikts? Der Einsatz automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger wegen Straftaten im Zusammenhang mit einer Versammlung sollte daher beschränkt werden auf Ermittlungen wegen Straftaten eines bestimmten Gewichts.[1103]

1099 Hierzu Kapitel II. B. I. 1. b) gg).
1100 Kapitel II. B. I. 1. d) cc).
1101 Kapitel II. A. II. 1. b).
1102 Kapitel II. B. II. 1. und 2.
1103 In diese Richtung auch Report of the 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, UN

Angemessen erscheint eine Beschränkung auf Straftaten von „auch im Einzelfall erheblicher Bedeutung" (vgl. §§ 100g Abs. 1 S. 1 Nr. 1, 100i Abs. 1, 100k Abs. 1 S. 1 StPO). Eine Straftat von erheblicher Bedeutung muss nach einhelliger Auffassung mindestens dem Bereich der mittleren Kriminalität zuzurechnen sein, den Rechtsfrieden empfindlich stören und dazu geeignet sein, das Gefühl der Rechtssicherheit der Bevölkerung erheblich zu beeinträchtigen.[1104]

IV. Umsetzung in einer Rechtsgrundlage

1. Regelungstechnik

a) Orientierung an der Regelungstechnik der KI-Verordnung nicht empfehlenswert

Eine Orientierung an der Regelungstechnik der KI-Verordnung mit Blick auf biometrische Fernidentifizierungssysteme ist nicht ratsam. Die Verordnung enthält eine einheitliche Definition und Regelung für alle biometrischen Fernidentifizierungssysteme (z. B. Gesichtserkennung, Gangerkennung). Welche Methoden der biometrischen Erkennung solche der „Fernidentifizierung" sind, ist aber nicht klar abzugrenzen;[1105] eine solche allgemeine Definition würde daher ohne Not Rechtsunsicherheit hervorrufen. Zudem werfen unterschiedliche Methoden unterschiedliche Probleme auf. Allein bei der Gesichtserkennung ergeben sich, wie diese Arbeit zeigt, eine Reihe spezifischer Risiken, die es als solche zu erkennen und zu regeln gilt.[1106] Eine allgemeine Rechtsgrundlage für biometrische Fernidentifizierung erscheint vor diesem Hintergrund nicht ratsam; automatisierte Gesichtserkennung sollte als eigene Maßnahme geregelt werden. Sofern in der Strafverfolgung ein Erfordernis der biometrischen Fernidentifizierung mit anderen Methoden (z. B. Stimmerkennung, Gangerkennung) besteht, sollten die jeweiligen Risiken zunächst ausführlich und differenziert untersucht und erst dann eine darauf zugeschnittene Rechtsgrundlage geschaffen werden.

Doc. A/HRC/44/24, 2020, 10 („Existing recordings should only be used for the identification of assembly participants who are suspects of serious crimes.").

1104 BVerfGE 103, 21 (34) mwN. Näher zum Begriff der Straftat von auch im Einzelfall erheblicher Bedeutung MüKoStPO/*Rückert*, 2. Aufl. 2023, StPO § 100g Rn. 57 ff.

1105 Kapitel I. C. I. 1.

1106 Siehe nur Kapitel III. B. II. 2. f) zu Folgeproblemen bei Wahllichtbildvorlagen.

Auch die pauschale Unterscheidung zwischen Echtzeit- und nachträglicher Erkennung in der KI-Verordnung sollte nicht als Regelungstechnik übernommen werden.[1107] Diese grobe Einordnung wird den Besonderheiten der einzelnen Einsatzvarianten nicht gerecht: Die Verwendung nachträglicher Gesichtserkennung zur Nachverfolgung des Weges eines Verdächtigen auf öffentlichen Videoaufzeichnungen birgt andere Gefahren als der Einsatz nachträglicher Gesichtserkennung zur Identifizierung unbekannter Verdächtiger anhand von Lichtbilddatenbanken. Jedes Einsatzszenario von Gesichtserkennung muss eigenständig betrachtet, vertieft untersucht und geregelt werden. Für den Einsatz automatisierter Gesichtserkennung gerade zum Zweck der Identifizierung unbekannter Verdächtiger sollte daher eine eigenständige Rechtsgrundlage geschaffen werden. Für die Verwendung automatisierter Gesichtserkennung in anderen Szenarien bedarf es zunächst weiterer vertiefter (u. a. rechtswissenschaftlicher) Untersuchungen.

b) Keine Ergänzung von § 98c StPO, sondern eigene Regelung

Der Einsatz automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger sollte nicht in § 98c StPO, sondern in einer eigenständigen Rechtsgrundlage geregelt werden. Die Maßnahme macht eine Vielzahl zusätzlicher Vorkehrungen nötig, die für einen „einfachen Datenabgleich", wie ihn § 98c StPO vorsieht, nicht erforderlich sind (z. B. Verwendung nur durch ausgebildete Lichtbildsachverständige und -experten, besondere technische Anforderungen an die verwendeten Systeme).

Die Vorgaben des Art. 10 JI-RL, § 48 BDSG (Erfordernis der „unbedingten Erforderlichkeit" der Datenverarbeitung sowie geeignete Schutzgarantien)[1108] sollten, soweit wie möglich, direkt in der Rechtsgrundlage, ansonsten anderweitig gesetzlich verankert werden. Nur wo dies nicht möglich oder sinnvoll erscheint (z. B. Erfordernis von Schulungen), sollte auf innerbehördliche Regelungen ausgewichen werden. Auch die Vorgabe des Art. 26 Abs. 10 Uabs. 3 S. 2 KI-VO („Es muss sichergestellt werden, dass die Strafverfolgungsbehörden keine ausschließlich auf der Grundlage der Ausgabe solcher Systeme zur nachträglichen biometrischen Fernidentifizierung beruhende Entscheidung, aus der sich eine nachteilige Rechtsfolge

1107 Siehe bereits *Hahn*, ZfDR 2023, 142, 155 ff., 161.
1108 Kapitel II. B. I. 2. b).

für eine Person ergibt, treffen.")[1109] sollte – auch wenn sie unmittelbar gilt (Art. 288 Abs. 2 AEUV) – direkt in der Rechtsgrundlage zum Einsatz automatisierter Gesichtserkennung verankert werden. Um die in einer Hinsicht darüberhinausgehenden Vorgaben des Art. 11 JI-RL zu wahren,[1110] sollte diese Formulierung um den Passus „*oder eine erhebliche Beeinträchtigung*" ergänzt werden.

2. Vorschlag für eine Formulierung

Die neue Rechtsgrundlage für den Einsatz automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger könnte als § 163h StPO in die Strafprozessordnung eingefügt werden und folgendermaßen lauten:

> **§ 163h StPO Identifizierung unbekannter Verdächtiger mit automatisierter Gesichtserkennung**
> (1) Zur Ermittlung der Identität unbekannter Verdächtiger dürfen Gesichtserkennungssysteme verwendet werden, die anhand biometrischer Merkmale Lichtbilder verarbeiten (automatisierte Gesichtserkennung), wenn dies unbedingt erforderlich ist. Ein Abgleich eines Lichtbilds des Verdächtigen darf nur mit Lichtbildern der [nähere Bezeichnung der Datenbanken] vorgenommen werden.
> (2) Weitere Ermittlungen gegen eine mit automatisierter Gesichtserkennung identifizierte Person sind nur zulässig, wenn zwei natürliche Personen unabhängig voneinander die Personenidentität oder den Verdacht der Personenidentität mit dem Verdächtigen festgestellt haben. Eine Entscheidung, aus der sich eine nachteilige Rechtsfolge für eine Person ergibt, darf nicht ausschließlich auf der Grundlage der Ausgabe eines Gesichtserkennungssystems getroffen werden.
> (3) Eine Maßnahme nach Absatz 1 und eine Feststellung nach Absatz 2 Satz 1 dürfen nur hierfür besonders qualifizierte Personen treffen.
> (4) Eine Maßnahme nach Absatz 1 darf nur durch das Gericht, bei Gefahr im Verzug auch durch die Staatsanwaltschaft angeordnet werden. In dem Antrag ist darzulegen, dass die mit der Maßnahme nach Absatz 1 und der Feststellung nach Absatz 2 Satz 1 betrauten Personen die erforderliche Qualifikation besitzen.

1109 Kapitel II. B. I. 1. d) cc).
1110 Kapitel II. B. I. 2. c).

(5) Dient die automatisierte Gesichtserkennung der Identifizierung eines Verdächtigen wegen einer im Zusammenhang mit einer Versammlung begangenen Tat, so ist dies nur bei einer Straftat von auch im Einzelfall erheblicher Bedeutung zulässig.
(6) Für eine Maßnahme nach Absatz 1 dürfen nur Gesichtserkennungssysteme verwendet werden, die nach dem jeweiligen Stand der Technik ein Höchstmaß an Genauigkeit aufweisen und entsprechend zertifiziert sind. Die Bundesregierung wird ermächtigt, durch Rechtsverordnung Regelungen zu treffen über
1. die für eine Zertifizierung zuständige, von den Strafverfolgungsbehörden unabhängige Stelle,
2. die technischen und organisatorischen Anforderungen an das Zertifizierungsverfahren und
3. die Dauer der Gültigkeit eines Zertifikats.

In § 101 Abs. 1 StPO sollte „§ 163h" ergänzt werden, sodass die Kennzeichnungs- und Löschpflichten auch für diese Vorschrift gelten.

In § 101 Abs. 4 („Von den in Absatz 1 genannten Maßnahmen sind im Falle […] zu benachrichtigen") sollte ergänzt werden: „Nr. 14 des § 163h die betroffene Person, gegen die nach Abgleich der Lichtbilder weitere Ermittlungen geführt wurden".

C. Weitere Empfehlungen

I. Schulungen und Überarbeitung der RiStBV

Um Fehler im Zusammenhang mit dem Einsatz automatisierter Gesichtserkennung so weit wie möglich zu verhindern, müssen Ermittler im Umgang mit den Ergebnissen von Gesichtserkennungsrecherchen geschult sein. Die Fehleranfälligkeit der Technologie[1111] und vor allem die Quellen menschlicher Fehler[1112] müssen ihnen bewusst sein. Zu diesem Zweck sollten etwa Fälle des Einsatzes automatisierter Gesichtserkennung, in denen (wie sich später herausstellte) gegen Unbeteiligte ermittelt wurde, herangezogen und daraufhin untersucht werden, ob und wie dies hätte verhindert werden können.

1111 Kapitel III. B. II. 1. und Kapitel I. E. IV.
1112 Kapitel III. B. II. 2. und 3.

Zudem wäre es ratsam, die RiStBV um spezifische Vorschriften zum Einsatz von Gesichtserkennung zu ergänzen. So könnte etwa in Nr. 18 RiStBV (Gegenüberstellung und Wahllichtbildvorlage) festgelegt werden, dass bei einer Gegenüberstellung oder Wahllichtbildvorlage dem Zeugen nicht offenbart werden darf, dass ursprünglich Gesichtserkennung zur Identifizierung des Verdächtigen verwendet wurde. Auch könnte in den RiStBV geregelt werden, dass zum Gesichtserkennungsabgleich nur Bilder des Verdächtigen (keine Doppelgänger; keine handgezeichneten oder computergenerierten zusammengesetzten Gesichtern auf der Grundlage von Zeugenbeschreibungen) verwendet werden dürfen.

II. Kontrolle und Evaluation

Der Einsatz automatisierter Gesichtserkennung kann unbeabsichtigte Folgen mit sich bringen, insbesondere für die Selektivität der Strafverfolgung und für Unbeteiligte, die Ermittlungsmaßnahmen unterworfen werden.[1113] Auch kann sich der Einsatz automatisierter Gesichtserkennung auf die Wahrnehmung der Strafverfolgungsbehörden in der Öffentlichkeit auswirken. Gesichtserkennung ist eine heimliche Maßnahme, die zumindest in den Medien mit Fehlern und Rassismus assoziiert wird;[1114] bei fehlender Transparenz und Akzeptanz der Maßnahmen könnte das Vertrauen in die Polizei womöglich sinken.

Um dem entgegenzuwirken, sollte eine Evaluationskommission eingesetzt werden, die den Einsatz automatisierter Gesichtserkennung kontrolliert und evaluiert.[1115] Die Kommission sollte pluralistisch und divers besetzt und insbesondere die Disziplinen Rechtswissenschaft, Kriminologie, Informatik, Soziologie und Psychologie sollten vertreten sein. Damit soll keine Kontrolle jeder Einzelmaßnahme, sondern vielmehr des „Systems" Gesichtserkennung als Ganzem ermöglicht werden. Beispielsweise könnte die Evaluationskommission untersuchen bzw. untersuchen lassen, ob und in welchen Fällen es im Zusammenhang mit Gesichtserkennung zu Ermittlungen gegen Unbeteiligte kommt und ob dies bei bestimmten Personengruppen häufiger vorkommt. (Diese Erkenntnisse können wiederum zur Schulung von Polizisten verwendet werden, um für Probleme zu sensibili-

1113 Kapitel III. A. und B.
1114 Kapitel III. C. III. 3. c) und Kapitel III. C. IV. 2.
1115 Kapitel II. A. I. 3. c) cc.) und Kapitel III. C. IV. 2.

sieren.) Auf Basis dieser Erkenntnisse könnte die Kommission Vorschläge dafür erarbeiten, wie Fehler in der Mensch-Maschine-Interaktion verhindert werden können. Wichtig erscheint zudem, empirisch erforschen zu lassen, welche Delikte und welche Menschen mit Gesichtserkennung verstärkt verfolgt werden. Auch könnte die Kommission verfolgen und analysieren lassen, wie der Einsatz von Gesichtserkennung durch die Polizei in der Bevölkerung wahrgenommen wird.

Eine solche Kontrolle und Evaluation auf einer Meta-Ebene würde dazu beitragen, unbeabsichtigte Auswirkungen des Einsatzes von Gesichtserkennung frühzeitig zu erkennen. Außerdem könnte eine solche unabhängige Überprüfung das Vertrauen der Bevölkerung in den polizeilichen Einsatz neuer Strafverfolgungstechnologien stärken.

III. Bericht für die Öffentlichkeit

Für die Öffentlichkeit sollte die Kommission zudem einen jährlichen Bericht über den Einsatz von Gesichtserkennung in der Strafverfolgung erarbeiten. Darin könnten die Befunde eigener Untersuchungen enthalten sein, aber auch Informationen der Zertifizierungsstelle zur Anzahl der eingesetzten Systeme und vor allem zu Fehleranfälligkeit und Verzerrungen. Mit einem solchen Bericht bestünde eine deutlich solidere Basis für eine demokratische Debatte über die Verwendung von Gesichtserkennung und ihre unbeabsichtigten Folgen, als dies derzeit der Fall ist. Gesichtserkennung würde, so die Hoffnung, weniger als dystopische Überwachungstechnologie wahrgenommen, die die Behörden „heimlich" einführen und verwenden, sondern als eine Maßnahme, die auf rechtlicher Grundlage eingesetzt und umfassend kontrolliert und evaluiert wird.

IV. Beobachtung technologischer und gesellschaftlicher Entwicklungen

Von Seiten des Gesetzgebers sollten der technologische Fortschritt und gesellschaftliche Veränderungen gerade mit Blick auf den Einsatz automatisierter Gesichtserkennung beobachtet werden.

So sollte etwa verfolgt werden, wie sich die Leistungsfähigkeit von Gesichtserkennungssystemen – insbesondere im Vergleich zu der von Menschen – entwickelt. Wie bereits erwähnt, sollte das Erfordernis der Überprüfung von Treffern einer Kandidatenliste durch Menschen allerdings

kritisch hinterfragt werden, wenn in Zukunft deutlich wird, dass die Technologie leistungsfähiger ist als (auch geschulte) Menschen. Denn dann würde das Auswählen des Verdächtigen aus der Kandidatenliste durch Lichtbildsachverständige oder -experten zu *mehr Fehlern* und *mehr Ermittlungen gegen Unschuldige* führen, als wenn nur der Top-1-Treffer des Gesichtserkennungssystems direkt an den Ermittler weitergeleitet würde. Mit Art. 14 Abs. 5 S. 1 KI-VO (wenn man ihn überhaupt als materielle Vorgabe begreift) wäre dies allerdings nur dann vereinbar, wenn die Ermittler eine „Ausbildung" („training") in der Anwendung des Systems haben.

Ob bzw. wann die Technologie tatsächlich leistungsfähiger ist als geschulte Menschen, muss jedoch noch weiter erforscht werden. Auch müsste eine solche Umstellung der Abläufe (Top-1-Treffer wird direkt an Ermittler weitergeleitet) erst recht äußerst kritisch untersucht, begleitet und evaluiert werden. Insbesondere wird sich die Frage stellen, wie ein Automation bias so weit wie möglich verhindert werden kann. Diese Frage stellt sich bei der Weiterleitung von nur einem Treffer mit noch höherer Dringlichkeit, als wenn – wie gegenwärtig der Fall – die Lichtbildexperten und -sachverständigen aus einer Liste den Kandidaten selbst eine Person aktiv auswählen müssen. Auch stellen sich Folgefragen für das Gerichtsverfahren: Gerade wenn ein Gesichtserkennungssystem tatsächlich besser als der Mensch ist, kann es zu Fällen kommen, in denen das Ergebnis eben nicht mehr von einem Menschen überprüft und nachvollzogen werden kann. Wenn das System – verlässlicher als der Mensch – dann eine Person als Verdächtigen identifiziert und sich bei den Ermittlungen keine anderen Beweise ergeben, kommt es für die Verurteilung entscheidend darauf an, ob es sich um den Verdächtigen handelt oder nicht. Kann das Ergebnis des Gesichtserkennungssystems dann tatsächlich auch als *Beweis* herangezogen werden statt nur als ermittlungsunterstützender Hinweis? Die Frage, wie in Gerichtsverfahren mit nicht erklärbaren Ergebnissen von KI-Systemen umzugehen ist, bedarf noch intensiver weiterer Forschung.

D. Schlusswort

„The real problem is not whether machines think
but whether men do."
– B. F. Skinner[1116]

Diese Arbeit versteht sich als Kritik eines unreflektierten Einsatzes wirkmächtiger neuer Technologien. Verfassungsrechtliche Grundsätze und das Bewusstsein für Risiken können dabei allzu schnell in den Hintergrund treten. Dabei besteht nicht nur die Gefahr, dass Menschen die Technologien ohne Berücksichtigung möglicher Folgen entwickeln und gedankenlos anwenden. Ebenso bedenklich ist es, wenn der Gesetzgeber die Einführung unbeachtet geschehen lässt. Die Entscheidung über die Verwendung folgenreicher neuer Technologien in der Strafverfolgung muss vom demokratisch legitimierten Gesetzgeber durchdacht und bewusst getroffen sein.

Mit Blick auf automatisierte Gesichtserkennung war dies jedoch nicht der Fall. Bereits seit 2008 setzt das BKA ein Gesichtserkennungssystem zur Identifizierung unbekannter Verdächtiger ein, Bundespolizei und Landespolizeibehörden haben nachgezogen. Einige Polizeibehörden schaffen sich mittlerweile eigene Systeme an. Jedes Jahr werden zehntausende Suchanfragen durchgeführt – Tendenz steigend. Diese Entwicklung hat sich vollzogen ohne demokratischen Diskurs, ohne Schaffung einer Rechtsgrundlage und ohne die Beteiligung von Rechtswissenschaft und Kriminologie.

Diese Arbeit hat das Anliegen, eine Debatte über die Regulierung automatisierter Gesichtserkennung in der Strafverfolgung anzustoßen. Damit ist auch die Hoffnung verbunden, dass mit Blick auf neue Technologien der Fokus weniger auf dystopische, weit entfernte Zukunftsszenarien gerichtet wird. Stattdessen sollten konkrete Risiken in den Blick genommen werden, die bereits jetzt für Menschen und die Gesellschaft als Ganze bestehen. Das Recht darf hier nicht untätig zusehen.

1116 *Skinner*, Contingencies of Reinforcement, 1969, Kap. 9.

Kapitel V. Thesen

1. Der Einsatz automatisierter Gesichtserkennung in der Strafverfolgung geht mit einem besonderen Gefährdungspotenzial einher, denn er betrifft viele Unbeteiligte (Streubreite), birgt ein spezifisches Fehlerrisiko (Fehleranfälligkeit), erfolgt ohne Wissen der Betroffenen (Heimlichkeit) und ermöglicht die einfache und schnelle Vernetzung verschiedener Informationen (Vernetzungsmöglichkeit), die einer Person persönlich und eindeutig zugeordnet werden können (Biometrie).[1117]
2. Die Verwendung automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger birgt eine spezifische Fehleranfälligkeit.[1118] Zwar besteht in Ermittlungsverfahren immer die Gefahr, dass Unschuldige betroffen sind, da sich die Maßnahmen gegen Verdächtige (und nicht gegen Verurteilte) richten. Gesichtserkennung erhöht jedoch die Wahrscheinlichkeit, dass gänzlich Unbeteiligte beschuldigt werden und dass der Fehler wegen großer optischer Ähnlichkeit von Täter und Beschuldigtem im Laufe des Ermittlungsverfahrens nicht frühzeitig erkannt wird.
3. Der Einsatz automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger begründet Eingriffe in das Recht auf informationelle Selbstbestimmung. Eigenständige Eingriffe sind die Erstellung der Embeddings, der Abgleich des Suchbilds mit allen Lichtbildern einer Datenbank sowie das Auftauchen in der Kandidatenliste.[1119]
4. Dem Abgleich und dem Auftauchen in der Kandidatenliste kommt ein erhebliches Eingriffsgewicht zu.[1120] Grund dafür sind vor allem die Heimlichkeit, Streubreite und Anlasslosigkeit, Anknüpfung an höchstpersönliche körperliche Merkmale und die drohenden Folgeeingriffe. Nachrangig können auch Einschüchterungseffekte und die grundsätzliche leichte Verknüpfbarkeit von Informationen durch Gesichtserkennung herangezogen werden. Auch die spezifische Fehleranfälligkeit von Gesichtserkennung wirkt eingriffserhöhend.

1117 Kapitel I. D. I.
1118 Kapitel I. D. I. 2.
1119 Kapitel II. A. I. 2. a) aa), bb) und cc).
1120 Kapitel II. A. I. 2. b).

5. Die Maßstäbe für die Bewertung der Eingriffsintensität von verdeckten Maßnahmen sollten weiterentwickelt und um die Kategorie der spezifischen Fehleranfälligkeit einer Maßnahme erweitert werden.[1121] Diese sollte als eigenes Kriterium eingriffserhöhend berücksichtigt werden.
6. Die nachträgliche Auswertung von Aufzeichnungen einer Versammlung per Gesichtserkennung, um unbekannte Verdächtige zu identifizieren, ist geeignet, Bürgerinnen und Bürger von künftigen Versammlungen abzuhalten. Dies muss wegen des objektiv-rechtlichen Gehalts der Versammlungsfreiheit auch bei der Ausgestaltung oder Auslegung einer strafprozessualen Rechtsgrundlage für Gesichtserkennung berücksichtigt werden.[1122]
7. Es existiert derzeit keine strafprozessuale Rechtsgrundlage für den Einsatz automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger.[1123]
8. Die in Praxis und Literatur herangezogene Vorschrift des § 98c StPO ist keine taugliche Ermächtigung.[1124] Sie ist materiell weitgehend und formell vollständig voraussetzungslos und wird auch mit Blick auf die Bestimmtheit und Normenklarheit nicht den Anforderungen gerecht, die eine Ermächtigung für den Einsatz automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger erfüllen muss. Der Zweck des maschinellen Datenabgleichs („zur Aufklärung einer Straftat") ist angesichts der Eingriffsintensität automatisierter Gesichtserkennung zu unbestimmt formuliert, die Art der Datenabfrage bzw. das technische Eingriffsinstrument (Gesichtserkennung) sind nicht ausreichend spezifiziert, die zum Abgleich zugelassenen Datenbanken sind nicht hinreichend begrenzt und die Verwendung höchstpersönlicher biometrischer Merkmale geht aus der Norm nicht hervor.
9. Automatisierte Gesichtserkennung birgt nicht nur das (nicht unkritisch zu sehende) Potenzial, dass in Zukunft mehr und mehr Delikte verfolgt und aufgeklärt werden können. Sie droht auch auf die ohnehin bestehende Selektivität der Strafverfolgung verstärkt einzuwirken.[1125] Die Technologie bewirkt eine Verschiebung der Strafverfolgungsressourcen hin zu Straftaten, die (insbesondere in der Öffentlichkeit) visuell wahrnehmbar und erfassbar sind. Zudem droht eine intensi-

1121 Kapitel II. A. I. 2. b) gg).
1122 Kapitel II. A. II. 1. b).
1123 Kapitel II. C.
1124 Kapitel II. C. I.
1125 Kapitel III. A.

vere Verfolgung von Bagatellkriminalität als bisher, insbesondere bei Wiederholungstätern. Eine solche Entwicklung sollte nicht unbemerkt voranschreiten, sondern kriminologisch untersucht und kritisch hinterfragt werden.

10. Beschränkungen der durchsuchbaren Datenbanken sind ambivalent zu sehen.[1126] Einerseits verringert eine Begrenzung die Streubreite der Gesichtserkennungsmaßnahme und die Anzahl der Personen, die potenziell als der unbekannte Verdächtige fehlidentifiziert werden könnten. Andererseits bewirkt die Beschränkung eine immer stärkere Verschiebung der Verfolgung hin zu Personen, die bereits in der Vergangenheit mit der Polizei interagiert haben oder die aus anderen Gründen in den durchsuchbaren Datenbanken gespeichert sind (z. B. Asylsuchende).
11. Der Einsatz automatisierter Gesichtserkennung kann Folgen – insbesondere Ermittlungsmaßnahmen – für gänzlich Unbeteiligte mit sich bringen. Die Ursache hierfür liegt in Fehlern der Technologie, aber auch in menschlichen Fehlern, die durch die Mensch-Maschine-Interaktion noch verstärkt werden.[1127] Die menschlichen Fähigkeiten zur Gesichtserkennung sind stärker begrenzt als häufig angenommen. Der Automation bias, also die menschliche Tendenz, sich zu sehr auf automatisierte Hilfsmittel zu verlassen, erhöht das Risiko, dass Fehler nicht erkannt werden. Dies muss bei einer Regulierung von Gesichtserkennung berücksichtigt werden, um Ermittlungen gegen Unbeteiligte so weit wie möglich zu verhindern.
12. Gesichtserkennung birgt die Gefahr, dass Fehlidentifizierungen im Rahmen von Wahllichtbildvorlagen und Gegenüberstellungen zunehmen.[1128] Die Technologie ist besonders gut darin, sehr ähnlich aussehende Personen zu finden. Wenn durch Gesichtserkennung eine dem Täter optisch stark ähnelnde Person identifiziert und verdächtigt wird, ist es für den Zeugen besonders schwierig zu erkennen, dass es sich nicht um den Täter handelt.
13. Die Fehler, die im Zusammenhang mit Gesichtserkennung zu den Festnahmen Unschuldiger in den USA geführt haben,[1129] können nicht nur auf Fehler der Technologie und schlechte Polizeiarbeit zurückgeführt werden. Menschliche Fehler waren entscheidend mitverantwort-

1126 Kapitel III. A. II. 1.
1127 Kapitel III. B. II.
1128 Kapitel III. B. II. 2. f) und 3.
1129 Kapitel III. B. I. 1.

lich,[1130] insbesondere wurden offensichtliche optische Unterschiede zwischen Täter und Verdächtigtem ignoriert.

14. In der medialen Debatte wird Gesichtserkennung als eine fehleranfällige und „rassistische" Technologie dargestellt.[1131] Fehler beim Einsatz automatisierter Gesichtserkennung werden vorrangig der Technologie, nicht den Menschen zugeschrieben. Die menschliche Verantwortung und ein möglicher Automation bias werden regelmäßig übersehen.
15. Das Phänomen, dass der Automation bias von Menschen in einem zweiten Schritt von den Medien übersehen wird, lässt sich unter dem Begriff *sekundärer* Automation bias zusammenfassen.[1132] Einer solchen verzerrten Wahrnehmung sollte der Gesetzgeber nicht unterliegen und daher Regelungen treffen, um auch menschliche Fehler bei der Interaktion mit Gesichtserkennungssystemen so weit wie möglich zu verhindern.

1130 Kapitel III. B. II. 2. und 3.
1131 Kapitel III. B. III. 3.
1132 Kapitel III. B. IV. 3.

Literaturverzeichnis

Alle Internetquellen wurden zuletzt am 21.1.2024 abgerufen. Für alle Internetquellen, für die dies möglich war, wurde ein dauerhaft verfügbarer Link (Permalink) erstellt.

Abdul-Rahman, Laila, Vertrauens- und Legitimitätsbrüche: Was bedeutet Rassismus durch die Polizei für die Gesellschaft?, in: Hunold, Daniela / Singelnstein, Tobias (Hrsg.), Rassismus in der Polizei – Eine wissenschaftliche Bestandsaufnahme, Wiesbaden 2022, 471-480.

Aden, Hartmut / Fährmann, Jan, Defizite der Polizeirechtsentwicklung und Techniknutzung, ZRP 2019, 175-178.

Albers, Marion, Informationelle Selbstbestimmung als vielschichtiges Bündel von Rechtsbindungen und Rechtspositionen, in: Friedewald, Michael / Lamla, Jörn / Roßnagel, Alexander (Hrsg.), Informationelle Selbstbestimmung im digitalen Wandel, Wiesbaden 2017, 11-35.

Albright, Thomas D. / Garrett, Brandon L., The Law and Science of Eyewitness Evidence, Boston University Law Review 2022, 511-629.

Amelung, Knut, Rechtsschutz gegen strafprozessuale Grundrechtseingriffe, Berlin 1976.

Anderson, Elisha, Controversial Detroit facial recognition got him arrested for a crime he didn't commit, Detroit Free Press v. 10.7.2020, abrufbar unter https://eu.freep.com/story/news/local/michigan/detroit/2020/07/10/facial-recognition-detroit-michael-oliver-robert-williams/5392166002/ [https://perma.cc/XD3Y-976R].

Arzt, Clemens / Eier, Jana, Zur Rechtmäßigkeit der Speicherung personenbezogener Daten in „Gewalttäter"-Verbunddateien des Bundeskriminalamts, DVBl 2010, 816-824.

Arzt, Clemens, Verbunddateien des Bundeskriminalamts – Zeitgerechte Flurbereinigung, NJW 2011, 352-354.

Arzt, Clemens, Polizeiliche Verarbeitung „besonderer Kategorien personenbezogener Daten" – Zur Umsetzung der Richtlinie (EU) 2016/680 in Deutschland, DÖV 2023, 991-1002.

Bacon, Francis, Meditationes, in: Spedding, James / Ellis, Robert Leslie / Heath, Douglas Denon (Hrsg.), The Works of Francis Bacon Vol. XIV, Bd. XIV, Boston 1863, 59-96.

Bäcker, Matthias, Grundrechtlicher Informationsschutz gegen Private, Der Staat 2012, 91-116.

Bäcker, Matthias, Kriminalpräventionsrecht – Eine rechtssetzungsorientierte Studie zum Polizeirecht, zum Strafrecht und zum Strafverfahrensrecht, Tübingen 2015.

Barker, Peter, Innocent man arrested after facial recognition failed again, Louisiana News v. 5.1.2023, abrufbar unter https://localtoday.news/la/innocent-man-arrested-after-facial-recognition-failed-again-108313.html [https://perma.cc/Y576-XUZA].

Barrett, Lindsey, Ban Facial Recognition Technologies for Children – And for Everyone Else, Boston University Journal of Science and Technology Law 2020, 223-285.

Barthe, Christoph / Gericke, Jan (Hrsg.), Karlsruher Kommentar zur Strafprozessordnung – mit GVG, EGGVG und EMRK, 9. Aufl., München 2023 (zitiert als: KK-StPO/*Bearbeiter*).

Bauer, Nikolaus / Gogoll, Jan / Zuber, Niina, Gesichtserkennung – Ein Diskussionsbeitrag zur Regulierung der Technologie, München 2021.

Baum, Matthew / Potter, Philip, The relationships between mass media, public opinion, and foreign policy: toward a theoretical synthesis, Annual Review of Political Science 2008, 39-65.

Becker, Jörg-Peter / Erb, Volker / Esser, Robert / Graalmann-Scheerer, Kirsten / Hilger, Hans / Ignor, Alexander, Löwe/Rosenberg Kommentar zur Strafprozessordnung, Band 3 Teil 1, 27. Aufl. 2019, Berlin 2019 (zitiert als: Löwe/Rosenberg/*Bearbeiter* StPO).

Benedict, T.J., The Computer Got It Wrong: Facial Recognition Technology and Establishing Probable Cause to Arrest, Washington & Lee Law Review 2022, 849-898.

Bentham, Jeremy, Panoptikum oder Das Kontrollhaus, aus dem Englischen übersetzt v. Hofbauer, A. L. (Originaltitel: Panopticon, or, The Inspection House, 1787), in: Welzbacher, C. (Hrsg.), Panoptikum oder Das Kontrollhaus, Berlin 2013, 7-109.

Bergmann, Jan / Dienelt, Klaus, Kommentar Ausländerrecht, 14. Aufl., München 2022 (zitiert als: Bergmann/Dienelt/*Bearbeiter*).

Bernsmann, Klaus / Jansen, Kirsten, Heimliche Ermittlungsmethoden und ihre Kontrolle – Ein systematischer Überblick, StV 1998, 217-231.

Bernzen, Anna K., Roboter als Richter? – Zur Automatisierung der Rechtsprechung, RDi 2023, 132-138.

Beulke, Werner, Kurze Freiheitsstrafen bei Bagatelldelikten? – Ein Plädoyer zugunsten einer restriktiven Auslegung von § 47 StGB, in: Hilgendorf, Eric / Rengier, Rudolf (Hrsg.), Festschrift für Wolfgang Heinz zum 70. Geburtstag am 23. April 2012, Baden-Baden 2012, 594-609.

Bhuiyan, Johana, Major camera company can sort people by race, alert police when it spots Uighurs, Los Angeles Times v. 9.2.2021, abrufbar unter https://www.latimes.com/business/technology/story/2021-02-09/dahua-facial-recognition-china-surveillance-uighur [https://perma.cc/W6SB-AD6S].

Bhuiyan, Johana, First man wrongfully arrested because of facial recognition testifies as California weighs new bills, The Guardian v. 27.4.2023, abrufbar unter https://www.theguardian.com/us-news/2023/apr/27/california-police-facial-recognition-software [https://perma.cc/3E62-5USC].

Bhuiyan, Johana, TechScape: 'Are you kidding, carjacking?' – The problem with facial recognition in policing, The Guardian v. 15.8.2023, abrufbar unter https://www.theguardian.com/newsletters/2023/aug/15/techscape-facial-recognition-software-detroit-porcha-woodruff-black-people-ai [https://perma.cc/7A38-C5EZ].

Birkel, Christoph / Church, Daniel / Erdmann, Anke / Hager, Alisa / Leitgöb-Guzy, Nathalie, Sicherheit und Kriminalität in Deutschland – SKiD 2020. Bundesweite Kernbefunde des Viktimisierungssurvey des Bundeskriminalamts und der Polizeien der Länder, Wiesbaden 2022.

Birkel, Christoph / Church, Daniel / Hummelsheim-Doss, Dina / Leitgöb-Guzy, Nathalie / Oberwittler, Dietrich, Der Deutsche Viktimisierungssurvey 2017. Opfererfahrungen, kriminalitätsbezogene Einstellungen sowie die Wahrnehmung von Unsicherheit und Kriminalität in Deutschland, Wiesbaden 2019.

Bledsoe, Woodrow Wilson, Proposal for a Study to Determine the Feasibility of a Simplified Face Recognition Machine, Palo Alto 1963.

Bledsoe, Woodrow Wilson, The Model Method in Facial Recognition, Technical Report PRI 15, Palo Alto 1964.

Bledsoe, Woodrow Wilson, Facial Recognition Project Report, Palo Alto 1964.

Bledsoe, Woodrow Wilson, I Had a Dream: AAAI Presidential Address, AI Magazine 1986, 57-61.

Bliesener, Thomas, Ausländer- und Zuwandererkriminalität – Expertise im Auftrag des Sachverständigenrats deutscher Stiftungen für Integration und Migration für das Jahresgutachten 2019, Hannover 2018.

Blozik, Michael, Subsidiaritätsklauseln im Strafverfahren, Göttingen 2012.

BMI/BMJ, Zweiter Periodischer Sicherheitsbericht, 2006.

Bohnsack, Ralf / Geimer, Alexander / Meuser, Michael (Hrsg.), Hauptbegriffe qualitativer Sozialforschung, 4. Aufl., Opladen & Toronto 2018 (zitiert als: *Bearbeiter*, in: Bohnsack/Geimer/Meuser, Hauptbegriffe qualitativer Sozialforschung).

Bomhard, David / Merkle, Marieke, Europäische KI-Verordnung – der aktuelle Kommissionsentwurf und praktische Auswirkungen, RDi 2021, 276-283.

Bonfadelli, Heinz / Friemel, Thomas, Medienwirkungsforschung, 6. Aufl., Konstanz 2017.

Borchard, Edwin M., Convicting the Innocent – Sixty-five Actual Errors of Criminal Justice, New York 1932.

Bragias, Adelaide / Hine, Kelly / Fleet, Robert, 'Only in our best interest, right?' Public perceptions of police use of facial recognition technology, Police Practice and Research 2021, 1637-1654.

Brauckmann, Michael / Busch, Christoph, Large Scale Database Search, in: Li, Stan Z. / Jain, Anil K. (Hrsg.), Handbook of Face Recognition, 2. Aufl., London, 2011, 639-653.

Braun Binder, Nadja / Egli, Catherine, Umgang mit Hochrisiko-KI-Systemen in der KI-VO, MMR 2024, 626-630.

Britz, Gabriele, Informationelle Selbstbestimmung zwischen rechtswissenschaftlicher Grundsatzkritik und Beharren des Bundesverfassungsgerichts, in: Hoffmann-Riem, Wolfgang (Hrsg.), Offene Rechtswissenschaft, Tübingen 2010, 561-596.

Britz, Gabriele, Grundrechtliche Schutzpflichten in bald 50 Jahren Rechtsprechung des BVerfG, NVwZ 2023, 1449-1458.

Brodowski, *Dominik,* Verdeckte technische Überwachungsmaßnahmen im Polizei- und Strafverfahrensrecht – Zur rechtsstaatlichen und rechtspraktischen Notwendigkeit eines einheitlichen operativen Ermittlungsrechts, Tübingen 2016.

Brosius-Gersdorf, Frauke (Hrsg.), Dreier Grundgesetz Kommentar, Bd. I, 4. Aufl. 2023 (zitiert als: Dreier GG/*Bearbeiter*).

Brüning, Janique, Der Richtervorbehalt – ein zahnloser Tiger? – Über die verfassungsrechtliche Notwendigkeit des Richtervorbehalts und seine Ineffizienz in der Praxis, ZIS 2006, 29-35.

Brüning, Janique, Der Richtervorbehalt im strafrechtlichen Ermittlungsverfahren, Baden-Baden 2005.

Bull, Hans Peter, Informationelle Selbstbestimmung – Vision oder Illusion?, 2. Aufl., Tübingen 2011.

Bundespolizei, Teilprojekt 1 „Biometrische Gesichtserkennung" des Bundespolizeipräsidiums im Rahmen der Erprobung von Systemen zur intelligenten Videoanalyse durch das Bundesministerium des Innern, für Bau und Heimat, das Bundespolizeipräsidium, das Bundeskriminalamt und die Deutsche Bahn AG am Bahnhof Berlin Südkreuz im Zeitraum vom 01.08.2017 - 31.07.2018, 2018, abrufbar unter https://www.bundespolizei.de/Web/DE/04Aktuelles/01Meldungen/2018/10/181011_abschlussbericht_gesichtserkennung_down.pdf;jsessionid=23655894F907F34AB9C3DA71D2C8A986.1_cid370?__blob=publicationFile&v=1.

Buolamwini, Joy / Gebru, Timnit, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, Proceedings of Machine Learning Research 2018, 1-15.

Büro für Technikfolgenabschätzung beim deutschen Bundestag, Emotionserkennung mittels künstlicher Intelligenz – Perspektiven und Grenzen von Technologien zur Analyse von Gesichtsbewegungen, Themenkurzprofil Nr. 48, abrufbar unter https://www.bundestag.de/resource/blob/848996/b0a0e4dc737c35ee2626cdf2ffc8d31d/Themenkurzprofil-048-data.pdf [https://perma.cc/47GA-RJN2].

Burrell, Jenna / Fourcade, Marion, The Society of Algorithms, Annual Review of Sociology 2021, 213-237.

Chibanguza, Kuuya / Kuß, Christian / Steege, Hans (Hrsg.), Künstliche Intelligenz: Recht und Praxis automatisierter und autonomer Systeme, Baden-Baden 2022 (zitiert als: Bearbeiter, in: Chibanguza/Kuß/Steege, Künstliche Intelligenz, 2022).

Chibanguza, Kuuya / Steege, Hans, Die KI-Verordnung – Überblick über den neuen Rechtsrahmen, NJW 2024, 1769-1775.

Citron, Danielle Keats, Technological Due Process, Washington University Law Review 2008, 1249-1313.

Classen, Claus Dieter, Kann eine gemeineuropäische Grundrechtsdogmatik entstehen?, EuR 2022, 279-302.

Clayton, James / Derico, Ben, Clearview AI used nearly 1m times by US police, it tells the BBC, BBC v. 27.3.2023, abrufbar unter https://www.bbc.com/news/technology-65057011 [https://perma.cc/Q97Q-YFPQ].

Coded Bias Discussion Guide 2021, abrufbar unter https://independentlens.s3.amazonaws.com/2200/10%20Coded%20Bias/Indie%20Lens%20Pop-Up/CODEDBIAS_DiscussionGuide.pdf [https://perma.cc/79PM-RZ2B].

Commission Nationale de l'Informatique et des Libertés (CNIL), Reconnaissance faciale – Pour un débat à la hauteur des enjeux, 2019, abrufbar unter https://www.cnil.fr/sites/default/files/atoms/files/reconnaissance_faciale.pdf [https://perma.cc/37CZ-M5SB].

Congressional Research Service, Facial Recognition Technology and Law Enforcement: Select Constitutional Considerations, 2020, abrufbar unter https://crsreports.congress.gov/product/pdf/R/R46541 [https://perma.cc/JB3Z-EPCC].

Coppock, Alexander / Ekins, Emily / Kirby, David, The Long-lasting Effects of Newspaper Op-Eds on Public Opinion, Quarterly Journal of Political Science 2018, 59-87.

Crespo, Andrew Manuel, The Hidden Law of Plea Bargaining, Columbia Law Review 2018, 1303-1424.

Crespo, Andrew Manuel, No Justice, No Pleas: Subverting Mass Incarceration Through Defendant Collective Action, Fordham Law Review 2022, 1999-2024.

Crummenerl, Jürgen, Sicherheitsstaat und Strafverteidigung, StV 1989, 131-133.

Cummings, Mary, Automation Bias in Intelligent Time Critical Decision Support Systems, AIAA 1st Intelligent Systems Technical Conference 2004, 1-6.

De Mot, Jef / Faure, Michael G., Public Authority Liability and the Chilling Effect, Tort Law Review 2014, 120-133.

Denham, Hannah, IBM's decision to abandon facial recognition technology fueled by years of debate, The Washington Post v. 11.6.2020, abrufbar unter https://www.washingtonpost.com/technology/2020/06/11/ibm-facial-recognition/# [https://perma.cc/2ENX-EA99].

Der Bayerische Landesbeauftragte für den Datenschutz, 31. Tätigkeitsbericht 2021, München 2022 (zitiert als: *Der Bayerische Landesbeauftragte für den Datenschutz*, Tätigkeitsbericht 2021).

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, 27. Tätigkeitsbericht 2018, Hamburg 2019 (zitiert als: *Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit*, Tätigkeitsbericht 2018).

Der Landesbeauftragte für den Datenschutz Rheinland- Pfalz, 22. Tätigkeitsbericht 2008-2009, 2010, LT-Drs. RP 15/4300.

Desoi, Monika, Intelligente Videoüberwachung – Rechtliche Bewertung und rechtsgemäße Gestaltung, Wiesbaden 2018.

Dietrich, Jan-Hendrich / Fahrner, Matthias / Gazeas, Nikolaos / von Heintschel-Heinegg, Bernd (Hrsg.), Handbuch Sicherheits- und Staatsschutzrecht, München 2022 (zitiert als: *Bearbeiter*, in: Dietrich/Fahrner/Gazeas/von Heintschel-Heinegg, Handbuch Sicherheits- und Staatsschutzrecht).

Diggelmann, Oliver, Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer (VVDStRL) 2011, 50-77.

Dölling, Dieter / Hermann, Dieter / Laue, Christian, Kriminologie – Ein Grundriss, Berlin 2022.

Dölling, Dieter, Polizeiliche Ermittlungstätigkeit und Legalitätsprinzip – Eine empirische und juristische Analyse des Ermittlungsverfahrens unter besonderer Berücksichtigung der Aufklärungs- und Verurteilungswahrscheinlichkeit – Erster Halbband, Wiesbaden 1987.

Donaubauer, Lena, Der polizeiliche Einsatz von Bodycams – Eine Untersuchung aus kriminologischer, verfassungsrechtlicher und menschenrechtlicher Perspektive, Frankfurt am Main 2017.

Dreier, Horst, Idee und Gestalt des freiheitlichen Verfassungsstaates, Tübingen 2014.

Dürig, Günter, Der Grundrechtssatz von der Menschenwürde. Entwurf eines praktikablen Wertsystems der Grundrechte aus Art. 1 Abs. I in Verbindung mit Art. 19 Abs. II des Grundgesetzes, AöR 1956, 117-157.

Ebeling, Christoph, Die organisierte Versammlung – Kontinuität zwischen Repression und Schutz, Berlin 2017.

Ebers, Martin / Heinze, Christian A. / Krügel, Tina / Steinrötter, Björn, Künstliche Intelligenz und Robotik, München 2020 (zitiert: Bearbeiter, in: Ebers/Heinze/Krügel/Steinrötter, Künstliche Intelligenz und Robotik).

Ebers, Martin / Hoch, Veronica / Rosenkranz, / Ruschemeier, Hannah / Steinrötter, Björn, Der Entwurf für eine EU-KI-Verordnung: Richtige Richtung mit Optimierungsbedarf, RDi 2021, 528-537.

Ebers, Martin, Explainable AI in the European Union: An Overview of the Current Legal Framework(s), in: Colonna, Liane / Greenstein, Stanley (Hrsg.), Nordic Yearbook of Law and Informatics 2020-2021 – Law in the Era of Artificial Intelligence, Visby 2022, 103-132.

Ebert, Andreas / Spiecker (gen. Döhmann), Indra, Der Kommissionsentwurf für eine KI-Verordnung der EU, NVwZ 2021, 1188-1193.

Eckstein, Ken, Ermittlungen zu Lasten Dritter, Tübingen 2013.

Eisenberg, Ulrich / Kölbel, Ralf, Kriminologie, 8. Aufl., Tübingen 2024.

Ensminger, Petra, „Immer mehr Überwachung um uns herum", Deutschlandfunk v. 11.12.2014, abrufbar unter https://www.deutschlandfunk.de/eugh-urteil-immer-mehr-ueberwachung-um-uns-herum-100.html [https://perma.cc/9DJZ-VQE7].

Epping, Volker / Hillgruber, Christian (Hrsg.), Beck'scher Online-Kommentar Grundgesetz, 56. Ed., Stand: 15.8.2023, München 2023 (zitiert als: BeckOK GG/*Bearbeiter*).

Ernst, Christian, Algorithmische Entscheidungsfindung und personenbezogene Daten, JZ 2017, 1026-1036.

Europäische Kommission, Weißbuch „Zur künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen", COM(2020) 65 final, 2020.

Europäischer Datenschutzausschuss, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, Version 2.0, 2023.

Facial Identification Scientific Working Group, Guidelines and recommendations for facial comparison training to competency, v. 18.11.2010, abrufbar unter https://fiswg.org/fiswg_training_guidelines_recommendations_v1.1_2010_11_18_archived.pdf [https://perma.cc/NL9B-KHNV].

Facial Recognition Motion (redigierte Version), National Association of Criminal Defense Lawyers, 13.11.2019, https://nacdl.org/getattachment/ac234f36-95d0-4b7c-8a0e-6bf422b5ecaf/redacted-facial-recognition-motion-8-28-18_flattened-5-.pdf [https://perma.cc/VMF4-DFEZ].

Fährmann, Jan, Kontrollieren? Aber warum, wann und wie? Kritische Perspektive auf polizeiliche Identitätsfeststellungen, in: Grafl, Christian / Stempkowski, Monika / Beclin, Katharina / Haider, Isabel (Hrsg.), „Sag, wie hast du's mit der Kriminologie?" – Die Kriminologie im Gespräch mit ihren Nachbardisziplinen, Mönchengladbach 2020, 643-660.

Fährmann, Jan, Digitale Beweismittel und Datenmengen im Strafprozess, MMR 2020, 228-233.

Ferguson, Andrew Guthrie, Facial Recognition and the Fourth Amendment, Minnesota Law Review 2021, 1105-1210.

Feuerhelm, Wolfgang, Polizei und „Zigeuner" – Strategien, Handlungsmuster und Alltagstheorien im polizeilichen Umgang mit Sinti u. Roma, Stuttgart 1987.

Feuerstack, Daniel / Becker, Daniel / Hertz, Nora, Die Entwürfe des EU-Parlaments und der EU-Kommission für eine KI-Verordnung im Vergleich, ZfDR 2023, 421-444.

Fisher, George, Plea Bargaining's Triumph, Yale Law Journal 2000, 857-1086.

Floridi, Luciano, The European Legislation on AI: a Brief Analysis of its Philosophical Approach, Philosophy & Technology 2021, 215-222.

Fossi, Connie / Prazan, Phil, Miami Police Used Facial Recognition Technology in Protester's Arrest, NBC MIAMI v. 17.8.2020, abrufbar unter https://www.nbcmiami.com/investigations/miami-police-used-facial-recognition-technology-in-protesters-arrest/2278848/ [https://perma.cc/H7HM-Y8N2].

Fox, Philip / Privitera, Daniel / Reuel, Anka, So denken die Deutschen über KI – KIRA Report, Zentrum für KI-Risken und -Auswirkungen, Berlin 2023.

Frankl, Sabine, Personenidentifizierung mittels Mensch und Maschine, Kriminalistik 2019, 130-136.

Frenz, Walter, Das Grundrecht auf informationelle Selbstbestimmung – Stand nach dem Antiterrordatei-Urteil des BVerfG, JA 2013, 840-845.

Friedman, Lawrence / Hansen, Victor, Secrecy, Transparency, and National Security, William Mitchell Law Review 2012, 1610-1628.

Friedrich, Lutz, Versammlungsinfrastrukturen: An den Grenzen des Versammlungsrechts, DÖV 2019, 55-64.

Galterio, Mary Grace / Shavit, Simi Angelic / Hayajneh, Thaier, A Review of Facial Biometrics Security for Smart Devices, Computers 2018, 1-11.

Garrett, Brandon L., Judging Innocence, Columbia Law Review 2008, 55-142.

Garvie, Clare / Bedoya, Alvaro / Frankle, Jonathan, The Perpetual Line-Up: Unregulated Police Face Recognition in America, Center on Privacy & Technology, Georgetown Law 2016 v. 18.10.2016, abrufbar unter https://www.perpetuallineup.org [https://perma.cc/BSF9-9A9C].

Garvie, Clare, Garbage in, garbage out, Center on Privacy & Technology Georgetown Law v. 16.5.2019, abrufbar unter https://www.flawedfacedata.com [https://perma.cc/J64B-MPQ8].

Garvie, Clare / Moy, Laura, America Under Watch: Face Surveillance in the United States, Center on Privacy & Technology, Georgetown Law v. 16.5.2019, abrufbar unter https://www.americaunderwatch.com [https://perma.cc/5A5T-DHYJ].

Garvie, Clare, ACLU News & Commentary v. 24.6.2020, abrufbar unter https://www.aclu.org/news/privacy-technology/the-untold-number-of-people-implicated-in-crimes-they-didnt-commit-because-of-face-recognition [https://perma.cc/TP78-XWC8].

Gates, Kelly, The Tampa 'Smart CCTV' Experiment, Culture Unbound Journal of Current Cultural Research 2010, 67-89.

Gates, Kelly, Identifying the 9/11 'Faces of Terror': The promise and problem of facial recognition technology, Cultural Studies 2006, 417-440.

Gazal-Ayal, Oren, Partial Ban on Plea Bargains, Cardozo Law Review 2006, 2295-2347.

Gelman, Andrew / Fagan, Jeffrey / Kiss, Alex, An Analysis of the New York City Police Department's "Stop-and-Frisk" Policy in the Context of Claims of Racial Bias, Journal of the American Statistical Association 2007, 813-823.

Geminn, Christian, Menschenwürde und menschenähnliche Maschinen und Systeme, DÖV 2020, 172-181.

Geminn, Christian, Die Regulierung Künstlicher Intelligenz, ZD 2021, 354-359.

General, John / Sarlin, Jon, A false facial recognition match sent this innocent Black man to jail, CNN Business v. 29.4.2021, abrufbar unter https://edition.cnn.com/2021/04/29/tech/nijeer-parks-facial-recognition-police-arrest/index.html [https://perma.cc/9PT6-HKD8].

Gercke, Björn / Temming, Dieter / Zöller, Mark A. (Hrsg.) Heidelberger Kommentar zur Strafprozessordnung, 7. Aufl., München 2023 (zitiert als: *Bearbeiter*, in: Gercke/Temming/Zöller).

Gerdemann, Simon, Harmonisierte Normen und ihre Bedeutung für die Zukunft der KI, MMR 2024, 614-621.

Gerhold, Maximilian, 40 Jahre CNIL – Ein Blick auf den französischen Gendarmen des Privatlebens DuD 2018, 368-372.

Gersdorf, Hubertus / Paal, Boris (Hrsg.), Beck'scher Online-Kommentar Informations- und Medienrecht, 42. Ed., Stand: 1.5.2021, München 2021 (zitiert als: BeckOK InfoMedienR/*Bearbeiter*).

Gilani, Syed Zulqarnain / Mian, Ajmal, Learning from Millions of 3D Scans for Large-scale 3D Face Recognition, Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition 2018, 1896-1905.

Gisch, Matthias, Datenschutzaufsicht im strafprozessualen Ermittlungsverfahren, KriPoZ 2020, 328-336.

Goddard, Kate / Roudsari, Abdul / Wyatt, Jeremy C., Automation bias: a systematic review of frequency, effect mediators, and mitigators, Journal of the American Medical Informatics Association 2012, 121-127.

Goel, Sharad / Rao, Justin M. / Shroff, Ravi, Precinct or Prejudice? Understanding Racial Disparities in New York City's Stop-and-Frisk Policy, Annals of Applied Statistics 2016, 365-394.

Götz, Volkmar, Polizeiliche Bildaufnahmen von öffentlichen Versammlungen – Zu den Neuregelungen in §§ 12a, 19a VersammlG, NVwZ 1990, 112-116.

Gola, Peter / Heckmann, Dirk (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, VO (EU) 2016/679 Kommentar, 3. Aufl., München 2022 (zitiert als: Gola/Heckmann/*Bearbeiter*).

Golla, Sebastian, In Würde vor Ampel und Algorithmus – Verfassungsrecht im technologischen Wandel, DÖV 2019, 673-681.

Golla, Sebastian, In Würde vor Ampel und Algorithmus – Verfassungsrecht im technologischen Wandel, in: Donath, Philipp / Bretthauer, Sebastian / Dickel-Görig, Marie / Drehwald, Jennifer / Gourdet, Sascha / Heger, Alexander / Henrich, Christina / Hoffmann, Julia / Kirchbach, Cornelia/ Kring, Jennifer / Lang, Lea Isabelle / Neumann, Theresa / Plicht, Sandra / Stix, Carolin / Völzmann, Berit / Wolckenhaar, Leonard (Hrsg.), Verfassungen – ihre Rolle im Wandel der Zeit. 59. Assistententagung Öffentliches Recht, Baden-Baden 2019.

Golla, Sebastian, Lernfähige Systeme, lernfähiges Polizeirecht. Regulierung von künstlicher Intelligenz am Beispiel von Videoüberwachung und Datenabgleich, KrimJ 2020, 149-161.

Golla, Sebastian, Algorithmen, die nach Terroristen schürfen – „Data-Mining" zur Gefahrenabwehr und zur Strafverfolgung, NJW 2021, 667-672.

Gong, Sixue / Liu, Xiaoming / Jain, Anil K., Reducing Bias in Face Recognition, in: Li, Stan Z. / Jain, Anil K. / Deng, Jiankang (Hrsg.), Handbook of Face Recognition, 3. Aufl., Cham 2024, 347-386.

Graf, Jürgen (Hrsg.), Beck'scher Online-Kommentar Strafprozessordnung, 49. Ed., Stand: 1.10.2023, München 2023 (zitiert als: BeckOK StPO/*Bearbeiter*).

Greene, Jay, Microsoft won't sell police its facial-recognition technology, following similar moves by Amazon and IBM, The Washington Post v. 11.6.2020, abrufbar unter https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/ [https://perma.cc/Q255-8FPL].

Grother, Patrick / Quinn, George / Ngan, Mei, Face In Video Evaluation (FIVE). Face Recognition of Non-Cooperative Subjects, 2017.

Grother, Patrick / Ngan, Mei / Hanaoka, Kayee, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, 2019.

Grother, Patrick / Ngan, Mei / Hanaoka, Kayee, Face Recognition Technology Evaluation (FRTE) Part 2: Identification, NISTIR 8271 Draft Supplement, 2023.

Guijarro Santos, Victoria, Nicht besser als nichts – Ein Kommentar zum KI-Verordnungsentwurf, ZfDR 2023, 23-42.

Gusy, Christoph, Überwachung der Telekommunikation unter Richtervorbehalt: Effektiver Grundrechtsschutz oder Alibi?, ZRP 2003, 275-278.

Gusy, Christoph, Sicherheitsgesetzgebung, KritV 2012, 247-269.

Gusy, Christoph / Eichenhofer, Johannes, Menschenwürde und Privatheitsschutz, in: Lorenzmeier, Stefan / Folz, Hans-Peter (Hrsg.), Recht und Realität – Festschrift für Christoph Vedder, Baden-Baden 2017, 132-157.

Hacker, Philipp, Teaching Fairness to Artificial Intelligence: Existing and Novel Strategies Against Algorithmic Discrimination Under EU Law, Common Market Law Review 2018, 1143-1186.

Hacker, Philipp / Wessel, Lauri, KI-Trainingsdaten nach dem Verordnungsentwurf für Künstliche Intelligenz, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz / Rostalski, Frauke (Hrsg.), Künstliche Intelligenz, Tübingen 2022, 53-70.

Hacker, Philipp / Berz, Amelie, Der AI Act der Europäischen Union – Überblick, Kritik und Ausblick, ZRP 2023, 226-229.

Hacker, Philipp, Comments on the Final Trilogue Version of the AI Act, Version: 23.1.2024, 2024, abrufbar unter https://www.europeannewschool.eu/images/chairs/hacker/Comments%20on%20the%20AI%20Act.pdf.

Häder, Michael, Empirische Sozialforschung – Eine Einführung, Wiesbaden 2015.

Härtel, Ines, Digitalisierung im Lichte des Verfassungsrechts – Algorithmen, Predictive Policing, autonomes Fahren, LKV 2019, 49-60.

Hahn, Johanna, Die Regulierung biometrischer Fernidentifizierung in der Strafverfolgung im KI-Verordnungsentwurf der EU-Kommission – Mit lückenhafter Regulierung gegen lückenlose Überwachung, ZfDR 2023, 142-163.

Harwell, Drew, FBI, ICE Find State Driver's License Photos Are a Gold Mine for Facial-Recognition Searches, The Washington Post v. 7.7.2019, abrufbar unter https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/ [https://perma.cc/74E9-MJ4R].

Hassemer, Winfried, Stellungnahme zum Entwurf eines Gesetzes zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität (OrgKGr), KJ 1992, 64-80.

Heath, Brad, Racial gap in U.S. arrest rates: 'Staggering disparity', USA TODAY v. 19.112014, abrufbar unter https://www.usatoday.com/story/news/nation/2014/11/18/ferguson-black-arrest-rates/19043207/ [https://perma.cc/5YQ8-T6WM].

Heghmanns, Michael, Die prozessuale Rolle der Staatsanwaltschaft, GA 2003, 433-450.

Heldt, Amélie P., Gesichtserkennung: Schlüssel oder Spitzel?, MMR 2019, 285-289.

Helmken, Dierk, Reform des Richtervorbehalts – Vom Palliativum zum effektiven Grundrechtsschutz, StV 2003, 193-198.

Herdegen, Matthias, Die Menschenwürde im Fluß des bioethischen Diskurses, JZ 2001, 773-779.

Herdegen, Matthias / Masing, Johannes / Poscher, Ralf / Gärditz, Klaus Ferdinand (Hrsg.), Handbuch des Verfassungsrechts, München 2021 (zitiert als: *Bearbeiter*, in: Herdegen/Masing/Poscher/Gärditz, Handbuch des Verfassungsrechts).

Herzog, Roman / Scholz, Rupert / Herdegen, Matthias / Klein, Hans H. (Hrsg.), Maunz, Theodor / Dürig, Günter (Begr.), Grundgesetz Kommentar, 102. EL August 2023, München 2023 (zitiert als: Dürig/Herzog/Scholz/*Bearbeiter*).

High Level Expert Group on Artificial Intelligence, Ethics guidelines for trustworthy AI, 8.4.2019.

High Level Expert Group on Artificial Intelligence, The Assessment List for Trustworthy Artificial Intelligence for self assessment (ALTAI), 17.7.2020.

Hilgendorf, Eric, Die mißbrauchte Menschenwürde, Jahrbuch für Recht und Ethik 1999, 137-158.

Hilgendorf, Eric, Problemfelder der Menschenwürdedebatte in Deutschland und Europa und die Ensembletheorie der Menschenwürde, Zeitschrift für Evangelische Ethik, 2013, 258-271.

Hilgendorf, Eric, Problem Areas in the Dignity Debate and the Ensemble Theory of Human Dignity, in: Grimm, Dieter / Kemmerer, Alexandra / Möllers, Christoph (Hrsg.), Human Dignity in Context – Explorations of a Contested Concept, 325-343, Baden-Baden 2018.

Hilgendorf, Eric, „Die Schuld ist immer zweifellos"? – Offene Fragen bei Tatsachenfeststellung und Beweis mit Hilfe „intelligenter" Maschinen, in: Fischer, Thomas (Hrsg.), Beweis, Baden-Baden 2019, 229-251.

Hilger, Hans, Neues Strafverfahrensrecht durch das OrgKG, NStZ 1992, 457-463.

Hill, Hermann / Kugelmann, Dieter / Martini, Mario (Hrsg.), Perspektiven der digitalen Lebenswelt, Baden-Baden 2017 (zitiert als: *Bearbeiter*, in: Hill/Kugelmann/Martini, Perspektiven der digitalen Lebenswelt, 2017).

Hill, Kashmir, The Secretive Company That Might End Privacy as We Know It, The New York Times v. 18.1.2020, abrufbar unter https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html [https://perma.cc/C4H9-NC6H].

Hill, Kashmir, Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match, The New York Times v. 6.1.2021, abrufbar unter https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html [https://perma.cc/N5SG-WSQ4].

Hill, Kashmir / Mac, Ryan, Thousands of Dollars for Something I Didn't Do, The New York Times v. 31.3.2023, abrufbar unter https://www.nytimes.com/2023/03/31/technology/facial-recognition-false-arrests.html [https://perma.cc/98M2-VMHT].

Hill, Kashmir, Your Face Belongs to Us, New York 2023.

Hoffmann, Hanna, Regulierung der Künstlichen Intelligenz – Fundamentalkritik am Verordnungsentwurf zur Regulierung der Künstlichen Intelligenz der EU-Kommission vom 21.4.2021, K&R 2021, 369-374.

Hoffmann, Hanna, Der nichtstaatliche Einsatz biometrischer Gesichtserkennungssysteme nach der DSGVO, Baden-Baden 2023.

Hofmann, Anja, Personenidentifizierung durch Zeugen im Strafverfahren – Anforderungen an die ordnungsgemäße Durchführung von Wiedererkennungsverfahren und Beurteilung des Beweiswerts von Identifizierungsleistungen unter besonderer Berücksichtigung rechtspsychologischer und kriminalistischer Aspekte, Berlin 2013.

Hornung, Gerrit, Der Personenbezug biometrischer Daten – Zugleich eine Erwiderung auf Saeltzer (DuD 2004, 218 ff.), DuD 2004, 429-431.

Hornung, Gerrit / Schindler, Stephan, Das biometrische Auge der Polizei, ZD 2017, 203-209.

Hornung, Gerrit / Schindler, Stephan, Datenschutz bei der biometrischen Gesichtserkennung, DuD 2021, 515-521.

Howard, John J. / Laird, Eli J. / Sirotin, Yevgeniy B. / Rubin, Rebecca E. / Tipton, Jerry L. / Vemury, Arun R., Evaluating Proposed Fairness Models for Face Recognition Algorithms, in: Rousseau, Jean Jacques / Kapralos, Bill (Hrsg.) Pattern Recognition, Computer Vision, and Image Processing. ICPR 2022 International Workshops and Challenges. ICPR 2022. Lecture Notes in Computer Science, Cham 2023, 431–447.

Huang, Junming / Cook, Gavin G. / Xie, Yu, Large-scale quantitative evidence of media impact on public opinion toward China, Humanities and Social Sciences Communications 2021, 1-8.

Huber, Peter / Voßkuhle, Andreas (Hrsg.), Kommentar Grundgesetz, Band 1: Präambel, Artikel 1–19, 8. Aufl., München 2024 (zitiert als: Huber/Voßkuhle/*Bearbeiter*).

Hufen, Friedhelm, Staatsrecht II – Grundrechte, 10. Aufl., München 2023.

Hunold, Daniela / Wegner, Maren, Rassismus und Polizei – Zum Stand der Forschung, Aus Politik und Zeitgeschichte 2020, 27-32.

Hunold, Daniela, Polizei im Revier – Polizeiliche Handlungspraxis gegenüber Jugendlichen in der multiethnischen Stadt, Berlin 2015.

Hurtz, Simon, Gesichtserkennung – Eine Technologie und ihre Gefahren, Süddeutsche Zeitung v. 22.1.2020, abrufbar unter https://www.sueddeutsche.de/wirtschaft/gesichtserkennung-eine-technologie-und-ihre-gefahren-1.4767141 [https://perma.cc/8SWN-5AWK].

Huxley, Aldous, Brave New World, London 1950.

Ikonomova, Violet, Duggan Defends Detroit's Use Of Facial Recognition After Wrongful Arrest, Deadline Detroit v. 25.6.2020, abrufbar unter https://www.deadlinedetroit.com/articles/25614/duggan_defends_facial_recognition_after_wrongful_arrest_of_black_man [https://perma.cc/C66N-D33W].

Isensee, Josef /Kirchhof, Paul (Hrsg.), Handbuch des Staatsrechts, Band VII, 3. Aufl., Heidelberg 2009 (zitiert als: *Bearbeiter*, in: Isensee/Kirchhof, Handbuch des Staatsrechts, Band VII).

Isensee, Josef /Kirchhof, Paul (Hrsg.), Handbuch des Staatsrechts, Band VIII, 3. Aufl., Heidelberg 2010 (zitiert als: *Bearbeiter*, in: Isensee/Kirchhof, Handbuch des Staatsrechts, Band VIII).

Jackson, Kaitlin, Challenging Facial Recognition Software in Criminal Court, The Champion 2019, 14-26.

Jahn, Matthias, Strafprozessuale Eingriffsmaßnahmen im Lichte der aktuellen Rechtsprechung des BVerfG – Unter besonderer Berücksichtigung der in BVerfGK 1-5 veröffentlichten Entscheidungen, NStZ 2007, 255-265.

Jain, Anil K. / Bolle, Ruud / Pankanti, Sharath, Introduction to Biometrics, in: Jain, Anil K. / Bolle, Ruud / Pankanti, Sharath (Hrsg.), Biometrics. Personal Identification in Networked Society, Boston 1999 (Fourth Printing 2002), 1-41.

Jandt, Silke, Biometrische Videoüberwachung – was wäre wenn …, ZRP 2018, 16-19.

Jarass, Hans Dieter, Kommentar Charta der Grundrechte der Europäischen Union unter Einbeziehung der sonstigen Grundrechtsregelungen des Primärrechts und der EMRK, 4. Aufl., München 2021.

Jarass, Hans Dieter / Pieroth, Bodo, Grundgesetz für die Bundesrepublik Deutschland: Kommentar, 17. Aufl., München 2022 (zitiert als: Jarass/Pieroth/*Bearbeiter*).

Johannes, Paul / Weinhold, Robert, Das neue Datenschutzrecht bei Polizei und Justiz, Baden-Baden 2018.

Johnson, Khari, How Wrongful Arrests Based on AI Derailed 3 Men's Lives, Wired v. 7.3.2022, abrufbar unter https://www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives/ [https://perma.cc/A37S-XVBY].

Johnson, Khari, Face Recognition Software Led to His Arrest. It Was Dead Wrong, Wired v. 28.2.2023, abrufbar unter https://www.wired.com/story/face-recognition-software-led-to-his-arrest-it-was-dead-wrong/ [https://perma.cc/2B2X-27RH].

Jordan, Frank, LKA: Gesichtserkennung in Zukunft so wichtig wie Fingerabdruck, Bayerischer Rundfunk v. 1.6.2021, abrufbar unter https://www.br.de/nachrichten/bayern/lka-gesichtserkennung-in-zukunft-so-wichtig-wie-fingerabdruck,SYt5R9p [https://perma.cc/7FQS-3WQS].

Kämmerer, Jörn Axel / Kotzur, Markus (Hrsg.), Münch, Ingo v. / Kunig, Philip (Begr.), Kommentar Grundgesetz, Band 1: Präambel bis Art. 69, 7. Aufl., München 2021 (zitiert als: v. Münch/Kunig-*Bearbeiter*).

Kahmen, Alexandra, Die Vorschriften zur Benachrichtigungspflicht gemäß § 101 IV-VI StPO und ihre praktische Umsetzung, Berlin 2017.

Kalbhenn, Jan Christopher, Designvorgaben für Chatbots, Deepfakes und Emotionserkennungssysteme: Der Vorschlag der Europäischen Kommission zu einer KI-VO als Erweiterung der medienrechtlichen Plattformregulierung, Zeitschrift für Urheber- und Medienrecht 2021, 663-674.

Kanade, Takeo, Picture Processing System by Computer Complex and Recognition of Human Faces, Kyoto 1973.

Karaboga, Murat / Frei, Nula / Ebbers, Frank / Rovelli, Sophia / Friedewald, Michael / Runge, Greta, Automatisierte Erkennung von Stimme, Sprache und Gesicht: Technische, rechtliche und gesellschaftliche Herausforderungen, Zürich 2022.

Karpenstein, Ulrich / Mayer, Franz C. (Hrsg.), Konvention zum Schutz der Menschenrechte und Grundfreiheiten: EMRK 3. Aufl., München 2022 (zitiert als: *Bearbeiter*, in: Karpenstein/Mayer).

Kasulis Cho, Kelly, Woman sues Detroit after facial recognition mistakes her for crime suspect, The Washington Post v. 7.8.2023, abrufbar unter https://www.washingtonpost.com/nation/2023/08/07/michigan-porcha-woodruff-arrest-facial-recognition/ [https://perma.cc/YMS7-8RL].

Kemelmacher-Shlizerman, Ira / Seitz, Steven M. / Miller, Daniel / Brossard, Evan, The megaface benchmark: 1 million faces for recognition at scale, Proceedings of the IEEE Conference of Computer Vision and Pattern Recognition 2016, 4873–4882.

Kerber, Matthias, Wenn es um Gesichter geht, schaut sie ganz genau hin, Der Guller v. 26.8.2023, abrufbar unter https://www.stadtanzeiger-ortenau.de/offenburg-stadt/c-panorama/wenn-es-um-gesichter-geht-schaut-sie-ganz-genau-hin_a91920 [https://perma.cc/WC3P-8QSM].

Kerr, Orin, The Mosaic Theory of the Fourth Amendment, Michigan Law Review 2012, 311-354.

Kinzig, Jörg, Knast für den Diebstahl einer Milchschnitte? – Grenzen der Verhängung kurzer Freiheitsstrafen bei Bagatelltaten wiederholt straffälliger Personen, in: Dölling, Dieter / Götting, Bert / Meier, Bernd-Dieter / Verrel, Torsten (Hrsg.), Festschrift für Heinz Schöch, Verbrechen – Strafe – Resozialisierung, Berlin 2010, 647-668.

Klare, Brendan F. / Li, Zhifeng / Jain, Anil K., Matching Forensic Sketches to Mugshot Photos, IEEE Transactions on Pattern Analysis and Machine Intelligence 2011, 639-646.

Klare, Brednan F. / Burge, Mark J. / Klontz, Joshua C. / R. Vorder Bruegge, Richard W. / Jain, Anil K., Face Recognition Performance: Role of Demographic Information, IEEE Transactions on Information Forensics and Security 2012, 1789-1801.

Kleinberg, Jon / Mullainathan, Sendhil / Raghavan, Manish, Inherent Trade-Offs in the Fair Determination of Risk Scores, 8th Innovations in Theoretical Computer Science Conference (ITCS 2017), Leibniz International Proceedings in Informatics (LIPIcs), Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Vol. 67, 2017, 1-13.

Klontz, Joshua C. / Jain, Anil K., A Case Study on Unconstrained Facial Recognition Using the Boston Marathon Bombings Suspects. Technical Report MSU-CSE-13-4, 2013, 1-8.

Kluth, Winfried / Heusch, Andreas (Hrsg.), Beck'scher Online-Kommentar Ausländerrecht, 39. Ed., Stand: 1.10.2023, München 2023 (zitiert als: BeckOK AuslR/*Bearbeiter*).

Knauer, Christoph (Hrsg.), Münchener Kommentar zur Strafprozessordnung, Band 3/1: §§ 333-499, München 2019 (zit.: MüKoStPO/*Bearbeiter*).

Knauer, Christoph / Kudlich, Hans / Schneider, Hartmut (Hrsg.), Münchener Kommentar zur Strafprozessordnung, Band 1: §§ 1-150, 2. Aufl., München 2023 (zit.: MüKoStPO/*Bearbeiter*).

Knauer, Christoph (Hrsg.), Münchener Kommentar zur Strafprozessordnung, Band 3/2: GVG, EGGVG, EMRK, EGStPO, EGStGB, ZSHG, StrEG, IGG, G 10, AO, München 2018 (zit.: MüKoStPO/*Bearbeiter*).

Knoche, Martin / Rigoll, Gerhard, Tackling Face Verification Edge Cases: In-Depth Analysis and Human-Machine Fusion Approach, 18th International Conference on Machine Vision and Applications (MVA) 2023, 1-8. [Preprint verfügbar unter https://arxiv.org/pdf/2304.08134.pdf].

Knoche, Martin / Hörman, Stefan / Rigoll, Gerhard, Susceptibility to Image Resolution in Face Recognition and Training Strategies to Enhance Robustness, Leibniz Transactions on Embedded Systems 2022, 1-19 [Preprint verfügbar unter https://arxiv.org/pdf/2107.03769.pdf].

Körffer, Barbara, Auswertung personenbezogener Daten für Strafverfolgung und Gefahrenabwehr – genügen die gesetzlichen Grundlagen zum Schutz des Rechts auf informationelle Selbstbestimmung?, Datenschutznachrichten (DANA) 2014, 146-150.

Kötter, Matthias / Nolte, Jakob, Was bleibt von der „Polizeifestigkeit des Versammlungsrechts"?, DÖV 2009, 399-406.

Koranyi, Johannes / Singelnstein, Tobias, Rechtliche Grenzen für polizeiliche Bildaufnahmen von Versammlungen, NJW 2011, 124-128.

Kostka, Genia / Steinacker, Léa / Meckel, Miriam, Between security and convenience: Facial recognition technology in the eyes of citizens in China, Germany, the United Kingdom, and the United States, Public Understanding of Science 2021, 671-690.

Kostka, Genia / Steinacker, Léa / Meckel, Miriam, Under big brother's watchful eye: Cross-country attitudes toward facial recognition technology, Government Information Quarterly 2023, 1-20.

Kracauer, Siegfried, The Challenge of Qualitative Content Analysis, The Public Opinion Quarterly 1952, 631-642.

Krasman, Susanne / Egbert, Simon, Predictive Policing – Eine ethnographische Studie neuer Technologien zur Vorhersage von Straftaten und ihre Folgen für die polizeiliche Praxis. Projektabschlussbericht, Hamburg 2019.

Kuckartz, Udo, Mixed Methods, Methodologie, Forschungsdesigns und Analyseverfahren, Wiesbaden 2014.

Kuckartz, Udo, Qualitative Inhaltsanalyse. Methoden, Praxis, Computerunterstützung, 4. Aufl. Weinheim & Basel 2018.

Kudlich, Hans, Mitteilung der Bewegungsdaten eines Mobiltelefons als Überwachung der Telekommunikation – Besprechung von BGH, NJW 2001, 1587, JuS 2001, 1165-1169.

Kühling, Jürgen / Buchner, Benedikt (Hrsg.), Kommentar zur Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG, 4. Aufl., München 2024 (zitiert als: Kühling/Buchner/*Bearbeiter*).

Kulick, Andreas, „Höchstpersönliches Merkmal" – Verfassungsrechtliche Maßstäbe der Gesichtserkennung, NVwZ 2020, 1622-1627.

Kumkar, Lea / Roth-Isigkeit, David, Erklärungspflichten bei automatisierten Datenverarbeitungen nach der DSGVO, JZ 2020, 277-86.

Kuteynikov, Dmitry / Izhaev, Osman / Lebedev, Valeria / Zenin, Sergey, Privacy in the realm of Artificial Intelligence Systems Application for Remote Biometric Identification (Originaltitel: Неприкосновенность частной жизни в условиях использования систем искусственного интеллекта для удаленной биометрической идентификации личности), Lex Russica. 2022, 121-131.

Kutscha, Martin, Rechtsschutzdefizite bei Grundrechtseingriffen von Sicherheitsbehörden, NVwZ 2003, 1296-1300.

Kutting, Isabelle M. / Amin, Naziar, Mit „Rasse" gegen Rassismus?, DÖV 2020, 612-617.

Larkin, Philip, Going, Going, in: Thwaite, Anthony (Hrsg.), Collected Poems, London 2014 (Original: 1988), 190.

Lauscher, Anne / Legner, Sarah, Künstliche Intelligenz und Diskriminierung, ZfDR 2022, 367-390.

Law Journal Editorial Board, Commentary, In Favor of Access to Facial Recognition Technology for Law Enforcement, New Jersey Law Journal, 26.4.2020, abrufbar unter https://www.law.com/njlawjournal/2020/04/26/in-favor-of-access-to-facial-recognition-technology-for-law-enforcement/?slreturn=20230401120750 [https://perma.cc/EE9A-XPP9].

Leisegang, Daniel, Kompromiss zu biometrischer Massenüberwachung gescheitert, netzpolitik.org v. 12.6.2023, abrufbar unter https://netzpolitik.org/2023/ki-verordnung-kompromiss-zu-biometrischer-massenueberwachung-gescheitert/ [https://perma.cc/4PNV-AMZ6].

Leupold, Andreas / Wiebe, Andreas / Glossner, Silke (Hrsg.), IT-Recht, 4. Aufl., München 2021 (zitiert als: Leupold/Wiebe/Glossner/*Bearbeiter*, IT-Recht).

Li, Stan Z. / Jain, Anil K., Introduction, in: Li, Stan Z. / Jain, Anil K. (Hrsg.), Handbook of Face Recognition, 2. Aufl., London 2011, 1-15.

Lilie, Hans, Verwicklungen im Ermittlungsverfahren – Überlegungen zur Stellung der Staatsanwaltschaft im Ermittlungsverfahren, ZStW 111 (1999), 807-826.

Linardatos, Dimitrios, Auf dem Weg zu einer europäischen KI-Verordnung – ein (kritischer) Blick auf den aktuellen Kommissionsentwurf, GPR 2022, 58-70.

Lisken, Hans / Denninger, Erhard (Hrsg.), Handbuch des Polizeirechts, 7. Aufl., München 2021 (zitiert als: *Bearbeiter*, in: Lisken/Denninger, Handbuch des Polizeirechts).

Ludyga, Hannes, Rasse als Rechtsbegriff?, NJW 2021, 911-914.

Luhmann, Niklas, Die Realität der Massenmedien, 5. Aufl., Wiesbaden 2017.

MacNaughton-Smith, Peter, The Second Code Toward (or Away from) an Empiric Theory of Crime and Delinquency, Journal of Research in Crime and Delinquency 1968, 97-198.

MacNaughton-Smith, Peter, Der zweite Code. Auf dem Wege zu einer (oder hinweg von einer) empirisch begründeten Theorie über Verbrechen und Kriminalität, in: Lüderssen, Klaus / Sack, Fritz (Hrsg.), Seminar: Abweichendes Verhalten II, Frankfurt am Main 1975, 197-212.

Makihara, Yasushi / Matovski, Darko S. / Nixon, Mark S. / Carter, John N. / Yagi, Yasushi, Gait recognition: databases, representations, and applications, Wiley Encyclopedia of Electrical and Electronics Engineering 2015, 1-15.

Malorny, Friederike, Datenschutz als Grenze KI-basierter Auswahlentscheidungen im Arbeitsrecht, RdA 2022, 170-178.

Malorny, Friederike, Auswahlentscheidungen durch künstlich intelligente Systeme – Datenschutzrechtliche Grenzen im Arbeitsrecht, JuS 2022, 289-296.

Mangold, Anna Katharina / Payandeh, Mehrdad (Hrsg.), Handbuch Antidiskriminierungsrecht, Tübingen 2022 (zitiert als: *Bearbeiter*, in: Mangold/Payandeh, Handbuch Antidiskriminierungsrecht).

Marsch, Nikolaus, Kontrafakturen und Cover-Versionen aus Karlsruhe – Anmerkungen zu den „Recht auf Vergessen"-Entscheidungen des Bundesverfassungsgerichts (6.11.2019, 1 BvR 16/13 und 1 BvR 276/17), ZEuS 2020, 597-625.

Marsch, Nikolaus / Rademacher, Timo, Generalklauseln im Datenschutzrecht – Zur Rehabilitierung eines zentralen Bausteins des allgemeinen Informationsverwaltungsrechts, Die Verwaltung, 2021, 1-35.

Martini, Mario, Algorithmen als Herausforderung für die Rechtsordnung, JZ 2017, 1017-1025.

Martini, Mario, Transformation der Verwaltung durch Digitalisierung, DÖV 2017, 443-455.

Martini, Mario, Gesichtserkennung im Spannungsfeld zwischen Sicherheit und Freiheit, NVwZ 2022, 30-31.

Martini, Mario, Gesichtserkennung im Spannungsfeld zwischen Sicherheit und Freiheit, NVwZ-Extra 1-2/2022, 1-16.

Martini, Mario / Thiessen, Bianca / Ganter, Jonas, Digitale Versammlungsbeobachtung – Verfassungs- und datenschutzrechtliche Grenzen der Versammlungsüberwachung im digitalen Zeitalter, Berlin 2023.

Martini, Mario / Botta, Jonas, KI-Aufsicht im föderalen Staat, MMR 2024, 630-638.

Martini, Mario / Wendehorst, Christiane (Hrsg.), KI-VO: Verordnung über Künstliche Intelligenz, Kommentar, München 2024 (zitiert als: *Bearbeiter*, in: Martini/Wendehorst, KI-VO).

Martini, Peter, Verfassungsrechtliche Anforderungen an Vorratsspeicherungen, in: Emmenegger, Sigrid / Wiedmann, Ariane (Hrsg.), Linien der Rechtsprechung des Bundesverfassungsgerichts – erörtert von den wissenschaftlichen Mitarbeitern, Berlin 2011, 301-326.

Masri, Lena, Facial recognition is helping Putin curb dissent with the aid of U.S. tech, Reuters v. 28.3.2023, abrufbar unter https://www.reuters.com/investigates/special-report/ukraine-crisis-russia-detentions/ [https://perma.cc/L7QD-B5UA].

Mayring, Philipp, Qualitative Inhaltsanalyse: Grundlagen und Techniken, 13. Aufl., Weinheim 2022.

McCullagh, Declan, Call It Super Bowl Face Scan I, Wired v. 2.1.2001, abrufbar unter https://www.wired.com/2001/02/call-it-super-bowl-face-scan-i/ [https://perma.cc/9ES3-7Q8W].

Meier, Bernd-Dieter, Bagatellkriminalität: Freiheitsstrafe ist keine Lösung, in: Bannenberg, Britta / Brettel, Hauke / Freund, Georg / Meier, Bernd-Dieter / Remschmidt, Helmut / Safferling, Christoph (Hrsg.), Festschrift für Dieter Rössner, Über allem: Menschlichkeit, Baden-Baden 2015, 304-320.

Meier, Bernd-Dieter, Kriminologie, 6. Aufl., München 2021.

Merten, Detlef / Papier, Hans-Jürgen (Hrsg.), Handbuch der Grundrechte, Bd. IV, Heidelberg 2011 (zitiert als: *Bearbeiter*, in: Merten/Papier, Handbuch der Grundrechte).

Merten, Detlef / Papier, Hans-Jürgen (Hrsg.), Handbuch der Grundrechte, Bd. V, Heidelberg 2013 (zitiert als: *Bearbeiter*, in: Merten/Papier, Handbuch der Grundrechte).

Meyer, Roland, Unsichtbare Gesichter – Zur Bildgeschichte der Gesichtserkennung, Regards Croisés 2020, 12-29.

Mineo, Liz, Reporter examines secretive firm whose product allows law enforcement, others to uncover your identify based on picture, The Harvard Gazette v. 26.10.2023, abrufbar unter https://news.harvard.edu/gazette/story/2023/10/how-facial-recognition-app-poses-threat-to-privacy-civil-liberties/ [https://perma.cc/38QG-HF26].

Möstl, Markus / Weiner, Bernhard (Hrsg.), Beck'scher Online-Kommentar Polizei- und Ordnungsrecht Niedersachsen, 29. Ed., Stand: 1.11.2023, München 2023 (zitiert als: *Bearbeiter*, in: Möstl/Weiner, BeckOK Polizei- und Ordnungsrecht Niedersachsen).

Mohapatra, Debabrata, Prisons directorate to introduce biometric tech to track inmates, The Times of India v. 7.4.2023, abrufbar unter https://timesofindia.indiatimes.com/city/bhubaneswar/prisons-directorate-to-introduce-biometric-tech-to-track-inmates/articleshow/99311330.cms [https://perma.cc/2724-HEGJ].

Mosier, Kathleen L. / Skitka, Linda J. / Burdick, Mark D. / Heers, Susan Tj., Automation Bias, Accountability, and Verification Behaviors, Proceedings of the Human Factors and Ergonomics Society Annual Meeting 1996, 204-208.

Mosier, Kathleen L. / Skitka, Linda J., Human Decision Makers and Automated Decision Aids: Made for Each Other?, in: Parasuraman, Raja / Mouloua, Mustapha (Hrsg.), Automation and Human Performance: Theory and Applications, New York 1996, 201-220.

Moy, Laura, Facing Injustice: How Face Recognition Technology May Increase the Incidence of Misidentifications and Wrongful Convictions, William & Mary Bill of Rights Journal 2021, 337-372.

Mozur, Paul, Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras, The New York Times v. 8.7.2018, abrufbar unter https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html [https://perma.cc/BC7A-GUN5].

Mozur, Paul, One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority, The New York Times v. 14.4.2019, abrufbar unter https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html [https://perma.cc/85V6-WAML].

Müller, Jan-Laurin, Algorithmische Entscheidungssysteme im Nichtdiskriminierungsrecht – Dogmatische Herausforderungen und konzeptionelle Perspektiven, in: Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz / Rostalski, Frauke (Hrsg.), Künstliche Intelligenz, Tübingen 2022, 205-249.

Müller, Kai, Strafverfahrensrecht für Polizeistudium und -praxis, Stuttgart & München 2023.

Müller, Marion, Kriminalität, Kriminalisierung und Wohnungslosigkeit – Eine qualitative Untersuchung, Diss. Univ. Siegen, 2006.

Mysegades, Jan, Keine staatliche Gesichtserkennung ohne Spezial-Rechtsgrundlage, NVwZ 2020, 852-856.

National Research Council, Identifying the Culprit – Assessing Eyewitness Identification, Washington D.C. 2014.

Nemitz, Paul, Künstliche Intelligenz und Demokratie – Die KI-VO – ein Akt demokratisch legitimierter digitaler Souveränität der EU, MMR 2024, 603-605.

Nettesheim, Martin, Der Schutzauftrag des Rechts, VVDStRL 2011, 7-43.

Neubacher, Frank, Kriminologie, 5. Aufl., Baden-Baden 2023.

Ng*uyen, Kien / Fookes, Clinton / Jillela, Raghavender / Sridharan, Sridha / Ross, Arun*, Long range iris recognition: A survey, Pattern Recognition 2017, 123-143.

Niemz, Johannes / Singelnstein, Tobias, Racial Profiling als polizeiliche Praxis, in: Hunold, Daniela / Singelnstein, Tobias (Hrsg.), Rassismus in der Polizei. Eine wissenschaftliche Bestandsaufnahme, Wiesbaden 2022, 337-358.

Nink, David, Justiz und Algorithmen – Über die Schwächen menschlicher Entscheidungsfindung und die Möglichkeiten neuer Technologien in der Rechtsprechung, Berlin 2021.

O'Connor, Sean, Biometrics and Identification after 9/11, Bender's Immigration Bulletin 2002, 150-173.

Odenthal, Hans J., Fehlerquellen der sequenziellen Wahllichtbildvorlage unter Verwendung computergenerierter Vergleichsbilder, StV 2012, 683-686.

Orssich, Irina, Das europäische Konzept für vertrauenswürdige Künstliche Intelligenz, EuZW 2022, 254-261.

Orwat, Carsten, Diskriminierungsrisiken durch Verwendung von Algorithmen, Berlin 2019.

Paal, Boris / Hüger, Jakob, Die KI-VO und das Recht auf menschliche Entscheidung, MMR 2024, 540-544.

Paal, Boris / Pauly, Daniel (Hrsg.), Kommentar Datenschutz-Grundverordnung Bundesdatenschutzgesetz: DS-GVO BDSG, 3. Aufl., München 2021 (zitiert als: Paal/Pauly/*Bearbeiter*).

Palmiotto, Francesca / Menéndez González, Natalia, Facial recognition technology, democracy and human rights, Computer Law & Security Review 2023, 1-6.

Parasuraman, Raja / Riley, Victor, Humans and Automation: Use, Misuse, Disuse, Abuse, Human Factors 1997, 230-253.

Park, Unsang / Jain, Anil K., Face Aging Modeling, in: Li, Stan Z. / Jain, Anil K. (Hrsg.), Handbook of Face Recognition, 2. Aufl., London 2011, 251-274.

Petri, Thomas, Biometrie in der polizeilichen Ermittlungsarbeit am Beispiel der automatisierten Gesichtserkennung, GSZ 2018, 144-148.

Phillips, P. Jonathon / Grother, Patrick / Micheals, Ross, Evaluation Methods in Face Recognition, in: Li, Stan Z. / Jain, Anil K. (Hrsg.), Handbook of Face Recognition, 2. Aufl., London 2011, 551-574.

Phillips, P. Jonathon / Jiang, Fang / Narvekar, Abhijit / Ayyad, Julianne / O'Toole, Alice J., Another-race Effect for face recognition algorithms, ACM Transactions on Applied Perception 2011, 1-11.

Pilniok, Arne, Unionsrechtliche Regulierung des Einsatzes von KI-Systemen in der öffentlichen Verwaltung, DÖV 2024, 581-592.

Popitz, Heinrich, Über die Präventivwirkung des Nichtwissens, in: Pohlmann, Friedrich / Eßbach, Wolfgang (Hrsg.), Popitz, Soziale Normen, Frankfurt am Main 2006 (Original: 1968), 158-174.

Poppe, Thorsten, Gesichtserkennung überprüft Stadionbesucher, Deutschlandfunk v. 18.8.2019, abrufbar unter https://www.deutschlandfunk.de/fussball-gesichtserkennung-ueberprueft-stadionbesucher-100.html [https://perma.cc/ZQ9X-CE8D].

Poscher, Ralf, Die Zukunft der informationellen Selbstbestimmung als Recht auf Abwehr von Grundrechtsgefährdungen, in: Gander, Hans-Helmuth / Perron, Walter / Poscher, Ralf / Riescher, Gisela /Würtenberger, Thomas (Hrsg.), Resilienz in der offenen Gesellschaft – Symposium des Centre for Security and Society, Baden-Baden 2012, 167-190.

Poscher, Ralf / Buchheim, Johannes, Staatsaufsicht und Datenschutz – Ein letzter weißer Fleck auf der datenschutzrechtlichen Landkarte?, DVBl 2015, 1273-1282.

Poscher, Ralf, Artificial Intelligence and the Right to Data Protection, in: Vöneky, Silja / Kellmeyer, Philipp / Müller, Oliver / Burgard, Wolfram (Hrsg.), The Cambridge Handbook of Responsible Artificial Intelligence, Cambridge 2022, 281-289.

Press, Eyal, Does A.I. Lead Police to Ignore Contradictory Evidence?, The New Yorker v. 13.11.2023, abrufbar unter https://www.newyorker.com/magazine/2023/11/20/does-a-i-lead-police-to-ignore-contradictory-evidence.

Przyborski, Aglaja / Wohlrab-Sahr, Monika, Qualitative Sozialforschung – Ein Arbeitsbuch, 5. Aufl., Berlin/Boston 2021.

Qian, Isabelle / Xiao, Muyi / Mozur, Paul / Cardia, Alexander, Four Takeaways From a Times Investigation Into China's Expanding Surveillance State, The New York Times v. 21.6.2022, abrufbar unter https://www.nytimes.com/2022/06/21/world/asia/china-surveillance-investigation.html [https://perma.cc/5MU8-T2PG].

Quach, Katyanna, Man wrongly jailed by facial recognition, lawyer claims, The Register v. 3.1.2023, abrufbar unter https://www.theregister.com/2023/01/03/facial_recognition_jail/ [https://perma.cc/LB93-YK96].

Rabinowicz, Carolina, Approaches to Regulating Government Use of Facial Recognition Technology, Harvard Journal of Law and Technology JOLT Digest v. 4.5.2023, abrufbar unter http://jolt.law.harvard.edu/digest/approaches-to-regulating-government-use-of-facial-recognition-technology [https://perma.cc/CU57-RQ9S].

Rademacher, Timo, Predictive Policing im deutschen Polizeirecht, AöR 2017, 366-416.

Rademacher, Timo, Wenn neue Technologien altes Recht durchsetzen: Dürfen wir es unmöglich machen, rechtswidrig zu handeln?, JZ 2019, 702-710.

Rademacher, Timo / Perkowski, Lennart, Staatliche Überwachung, neue Technologien und die Grundrechte, JuS 2020, 713-720.

Rademacher, Timo, Verdachtsgewinnung durch Algorithmen. Maßstäbe für den Einsatz von predictive policing und retrospective policing bei Gefahrenabwehr bzw. Strafverfolgung, in: Zimmer, Daniel (Hrsg.), Regulierung für Algorithmen und Künstliche Intelligenz, Baden-Baden 2021, 229-268.

Radtke, Tristan, Das Verhältnis von KI-VO und Art. 22 DS-GVO unter besonderer Berücksichtigung der Schutzzwecke, RDi 2024, 353-360.

Rampe, Henrik, Super-Recognizer: „Ich bin eher ein Ohrenfreund", ZEIT Online v. 24.10.2023, abrufbar unter https://www.zeit.de/zeit-verbrechen/2023/23/super-recognizer-talent-gesichter-erkennen-polizei-gedaechtnis [https://perma.cc/BFK8-7VRU].

Ramsthaler, Frank / Federspiel, Jan M. / Huckenbeck, Wolfgang / Kettner, Mattias / Lux, Constantin / Verhoff, Marcel A., Die forensische Gesichtserkennung anhand von Lichtbildern – Kann Amazons Rekognition (AWS) die Identifizierungssicherheit erhöhen?, Archiv für Kriminologie 2024, Band 254, 1-43.

Raposo, Vera Lúcia, The Use of Facial Recognition Technology by Law Enforcement in Europe: A Non-Orwellian Draft Proposal, European Journal on Criminal Policy and Research 2022, 515-533.

Raviv, Shaun, The Secret History of Facial Recognition, Wired v. 21.1.2020, abrufbar unter https://www.wired.com/story/secret-history-facial-recognition/ [https://perma.cc/A7YR-RLDT].

Reichertz, Jo, Die Macht der Worte und der Medien, 2. Aufl., Wiesbaden 2009.

Renan, Daphna, The Fourth Amendment as Administrative Governance, Stanford Law Review 2016, 1039-1129.

Ricker, Daniel, Anfangsverdacht und Vorurteil – Eine strafprozessrechtliche Untersuchung, Berlin 2021.

Riess, Peter, Über Subsidiaritätsverhältnisse und Subsidiaritätsklauseln im Strafverfahren, in: Geppert, Klaus / Dehnicke, Diether (Hrsg.), Gedächtnisschrift für Karlheinz Meyer, Berlin 1990, 367-390.

Roggan, Fredrik, Der Einsatz von Video-Drohnen bei Versammlungen, NVwZ 2011, 590-595.

Roggan, Fredrik, Die „Technikoffenheit" von strafprozessualen Ermittlungsbefugnissen und ihre Grenzen – Die Problematik der Auslegung von Gesetzen über ihren Wortlaut oder Wortsinn hinaus, NJW 2015, 1995-1999.

Roos, Philipp / Weitz, Caspar Alexander, Hochrisiko-KI-Systeme im Kommissionsentwurf für eine KI-Verordnung, MMR 2021, 844-851.

Ross, Arun / Jain, Anil K., Introduction to Biometrics, in: Jain, Anil K. / Flynn, Patrick / Ross, Arun A., Handbook of Biometrics, New York 2008, 1-22.

Rostalski, Frauke / Weiss, Erik, Der KI-Verordnungsentwurf der Europäischen Kommission, ZfDR 2021, 329-357.

Rostalski, Frauke / Weiss, Erik, Verbotene KI-Praktiken (Art. 5 KI-VO-E), in: Hilgendorf, Eric / Roth-Isigkeit, David (Hrsg.), Die neue Verordnung der EU zur Künstlichen Intelligenz, Technische Grundlagen, Rechtsprobleme, Rechtsfolgen, München 2023, 35-50.

Roth-Isigkeit, David, Der risikobasierte Ansatz als Paradigma des Digitalverwaltungsrechts – Die KI-VO im Kontext europäischer Risikoregulierung, MMR 2024, 621-626.

Rückert, Christian / Goger, Thomas, Neue Waffe im Kampf gegen Kinderpornografie im Darknet, MMR 2020, 373-378.

Rückert, Christian, Mit künstlicher Intelligenz auf Verbrecherjagd: Einsatz von Gesichtserkennungstechnologie zur Aufklärung der „Kapitolverbrechen", Verfassungsblog v. 22.1.2021, abrufbar unter https://verfassungsblog.de/ki-verbrecherjagd/ [https://perma.cc/B567-XXZN].

Rückert, Christian, Digitale Daten als Beweismittel im Strafverfahren, Tübingen 2023.

Russell, Jon, China's CCTV surveillance network took just 7 minutes to capture BBC reporter, TechCrunch v. 14.12.2017, abrufbar unter https://techcrunch.com/2017/12/13/china-cctv-bbc-reporter/#:~:text=It%20took%20Chinese%20authorities%20just,forcibly%20removed%20from%20the%20country [https://perma.cc/VM6Q-4YAJ].

Russell, Richard / Duchaine, Brad / Nakayama, Ken, Super-recognizers: People with extraordinary face recognition ability, Psychonomic Bulletin & Review 2009, 252-257.

Russell, Stuart / Norvig, Peter, Artificial Intelligence – A Modern Approch, 4. Aufl., Harlow 2022.

Safferling, Christoph / Rückert, Christian, Europäische Grund- und Menschenrechte im Strafverfahren – ein Paradigmenwechsel?, NJW 2021, 287-292.

Saldern, Matthias v., Qualitative Forschung – quantitative Forschung: Nekrolog auf einen Gegensatz. Empirische Pädagogik 1992, 377-399.

Satariano, Adam / Hill, Kashmir, Barred From Grocery Stores by Facial Recognition, The New York Times v. 28.6.2023, abrufbar unter https://www.nytimes.com/2023/06/28/technology/facial-recognition-shoplifters-britain.html [https://perma.cc/9BZB-AZL9].

Satzger, Helmut / Schluckebier, Wilhelm / Widmaier, Gunter (Hrsg.), StPO-Kommentar, 5. Aufl., Hürth 2023 (zitiert als: Satzger/Schluckebier/Widmaier/*Bearbeiter*, StPO-Kommentar).

Schantz, Peter / Wolff, Heinrich Amadeus, Das neue Datenschutzrecht, München 2017.

Schenk, *Michael,* Medienwirkungsforschung, 3. Aufl., Tübingen 2007.

Schindler, Stephan, Biometrische Videoüberwachung – Zur Zulässigkeit biometrischer Gesichtserkennung in Verbindung mit Videoüberwachung zur Bekämpfung von Straftaten, Baden-Baden 2021.

Schindler, Stephan, EU-Kommission: Verordnungsentwurf zur Regulierung von KI – Das Ende polizeilicher Gesichtserkennung im öffentlichen Raum?, ZD-Aktuell 2021, 05221.

Schindler, Stephan / Schomberg, Sabrina, Der KI-Verordnungsentwurf und biometrische Erkennung: Ein großer Wurf oder kompetenzwidrige Symbolpolitik?, in: Friedewald, Michael / Roßnagel, Alexander / Heesen, Jessica / Krämer, Nicole / Lamla, Jörn (Hrsg.), Künstliche Intelligenz, Demokratie und Privatheit, Baden-Baden 2022, 103-130.

Schmidt, Frank, Polizeiliche Videoüberwachung durch den Einsatz von Bodycams, Baden-Baden 2018.

Schmidt, Thomas, Wenn Partybilder helfen, Tatverdächtige zu finden, Süddeutsche Zeitung v. 4.5.2018, abrufbar unter https://www.sueddeutsche.de/muenchen/taeterermittlungen-fahndung-per-mausklick-1.3967846 [https://perma.cc/WAB6-F4EW].

Schneier, Bruce, The Coming AI Hackers, 2021, abrufbar unter https://www.belfercenter.org/sites/default/files/2021-04/HackingAI.pdf [https://perma.cc/3B3C-X5CZ].

Schreier, Margrit, Varianten qualitativer Inhaltsanalyse: ein Wegweiser im Dickicht der Begrifflichkeiten, Forum Qualitative Sozialforschung 2014, 1-27.

Schroff, Florian / Kalenichenko, Dmitry / Philbin, James, FaceNet: A unified embedding for face recognition and clustering, Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition 2015, 815-823.

Schünemann, Bernd, Wohin treibt der deutsche Strafprozess?, ZStW 114 (2002), 1-62.

Schwabenbauer, Thomas, Heimliche Grundrechtseingriffe – Ein Beitrag zu den Möglichkeiten und Grenzen sicherheitsbehördlicher Ausforschung, 2013 Tübingen.

Schweer, Thomas / Strasser, Hermann / Zdun, Steffen, „Das da draußen ist ein Zoo, und wir sind die Dompteure" – Polizisten im Konflikt mit ethnischen Minderheiten und sozialen Randgruppen, Wiesbaden 2008.

Schweer, Thomas / Strasser, Hermann, Die Polizei – dein Freund und Helfer, in: Groenemeyer, Axel / Mansel, Jürgen (Hrsg.), Die Ethnisierung von Alltagskonflikten, Wiesbaden 2003, 229-260.

Schwichtenberg, Simon, Das neue BDSG und die StPO: zwei, die bislang noch nicht zusammengefunden haben, NK 2020, 91-105.

Selinger, Evan / Hartzog, Woodrow, The Inconsentability of Facial Surveillance, Loyola Law Review 2019, 101-122.

Semerád, Lukáš / Drahanský, Martin, Retinal Vascular Characteristics in: Uhl, Andreas / Busch, Christoph / Marcel, Sébastien / Veldhuis, Raxmond (Hrsg.), Handbook of Vascular Biometrics, Cham 2020, 309-354.

Siebrecht, Michael, Ist der Datenabgleich zur Aufklärung einer Straftat rechtmäßig?, StV 1996, 566-570.

Siebrecht, Michael, Rasterfahndung – Eine EDV-gestützte Massenfahndungsmethode im Spannungsfeld zwischen einer effektiven Strafverfolgung und dem Recht auf informationelle Selbstbestimmung, Berlin 1997.

Simitis, Spiros / Hornung, Gerrit /Spiecker gen. Döhmann, Indra (Hrsg.), Datenschutzrecht, DSGVO mit BDSG, Baden-Baden 2019 (zitiert als: *Bearbeiter*, in: Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht).

Simitis, Spiros (Hrsg.), Kommentar Bundesdatenschutzgesetz, 8. Aufl., Baden-Baden 2014, (zitiert als: *Bearbeiter*, Bundesdatenschutzgesetz).

Singelnstein, Tobias, Möglichkeiten und Grenzen neuerer strafprozessualer Ermittlungsmaßnahmen – Telekommunikation, Web 2.0, Datenbeschlagnahme, polizeiliche Datenverarbeitung & Co, NStZ 2012, 593-606.

Singelnstein, Tobias, Sieben Thesen zu Entwicklung und Gestalt des Strafrechts, ZfR 2014, 321-329.

Singelnstein, Tobias, Predictive Policing: Algorithmenbasierte Straftatprognosen zur vorausschauenden Kriminalintervention, NStZ 2018, 1-9.

Singelnstein, Tobias, Strafbare Strafverfolgung – Voraussetzungen und Grenzen der Strafbarkeit von Amtsträgern sowie von strafprozessualen Amtsbefugnissen gemäß dem Prinzip der Prozessrechtsakzessorietät, Baden-Baden 2019.

Singelnstein, Tobias / Kunz, Karl-Ludwig, Kriminologie – Eine Grundlegung, 8. Aufl., Bern 2021.

Singer, Natasha, Amazon's Facial Recognition Wrongly Identifies 28 Lawmakers, A.C.L.U. Says, The New York Times v. 26.7.2018, abrufbar unter https://www.nytimes.com/2018/07/26/technology/amazon-aclu-facial-recognition-congress.html [https://perma.cc/4BP3-HHV8].

Sirovich, Lawrence / Kirby, Michael, Low-dimensional procedure for the characterization of human faces, Journal of the Optical Society of America 1987, 519–524.

Skinner, Burrhus Frederic, Contingencies of Reinforcement: A Theoretical Analysis, 1969, Version 2013 der B. F. Skinner Foundation.

Skitka, Linda J. / Mosier, Kathleen L. / Burdick, Mark, Does automation bias decision-making?, International Journal of Human-Computer Studies 1999, 991-1006.

Sklansky, David, Too Much Information: How Not to Think About Privacy and the Fourth Amendment, California Law Review 2014, 1069-1121.

Slevin, Peter, Police Video Cameras Taped Football Fans, The Washington Post v. 1.2.2001, abrufbar unter https://www.washingtonpost.com/archive/politics/2001/02/01/police-video-cameras-taped-football-fans/32b34d5d-7adb-4350-8fef-48a42bb55447/ [https://perma.cc/CMH5-YGJV].

Snow, Jacob, ACLU News & Commentary v. 26.7.2018, Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots, abrufbar unter https://www.aclu.org/news/privacy-technology/amazons-face-recognition-falsely-matched-28 [https://perma.cc/D847-DUG5].

Sofiotis, Ilias I., Grundrechtliche Würdigung des Einsatzes von Biometrie im Bereich der Strafverfolgung und im Strafverfahren, VR 2010, 186-190.

Soiné, Michael, Strafprozessordnung, 144. Lieferung, Heidelberg 2023 (zitiert als: *Soiné,* StPO).

Solopov, Maxim, На митинге в Москве полицейские обошлись без массовых задержаний. Но пришли к протестующим и журналистам сразу после – силовикам помогла система распознавания лиц, Meduza v. 27.4.2021, abrufbar unter https://meduza.io/feature/2021/04/27/na-mitinge-v-moskve-politseyskie-oboshlis-bez-massovyh-zaderzhaniy-zato-prishli-k-protestuyuschim-i-zhurnalistam-srazu-posle-pomogli-zapisi-s-kamer-videonablyudeniya, [https://perma.cc/KD8C-BCGJ].

Solove, Daniel, Access and Aggregation: Public Records, Privacy and the Constitution, Minnesota Law Review 2002, 1137-1209.

Sommerer, Lucia M., Personenbezogenes Predictive Policing – Kriminalwissenschaftliche Untersuchung über die Automatisierung der Kriminalprognose, Baden-Baden 2020.

Specht, Louisa / Mantz, Reto (Hrsg.), Handbuch Europäisches und deutsches Datenschutzrecht, München 2019 (zitiert als: *Bearbeiter*, in: Specht/Mantz, Handbuch Europäisches und deutsches Datenschutzrecht).

Spindler, Gerald, Der Vorschlag der EU-Kommission für eine Verordnung zur Regulierung der Künstlichen Intelligenz (KI-VO-E) – Ansatz, Instrumente, Qualität und Kontext, Computer und Recht 2021, 361-374.

Staben, Julian, Der Abschreckungseffekt auf die Grundrechtsausübung – Strukturen eines verfassungsrechtlichen Arguments, Tübingen 2016.

Stadler, Thomas, Der Richtervorbehalt – ein stumpfes Schwert oder ein rechtsstaatlich gebotenes Instrument?, ZRP 2013, 179-180.

Steege, Hans, Algorithmenbasierte Diskriminierung durch Einsatz von Künstlicher Intelligenz, MMR 2019, 715-721.

Steger, Thomas, Einführung in die qualitative Sozialforschung, Chemnitz 2003.

Steinbach, Kathrin, Regulierung algorithmenbasierter Entscheidungen – Grundrechtliche Argumentation im Kontext von Artikel 22 DSGVO, Berlin 2021.

Stern, Klaus / Sodan, Helge / Möstl, Markus (Hrsg.), Das Staatsrecht der Bundesrepublik Deutschland im europäischen Staatenverbund, 2. Aufl., München 2022 (zitiert als: *Bearbeiter*, in: Stern/Sodan/Möstl, Das Staatsrecht der Bundesrepublik Deutschland im europäischen Staatenverbund).

Stettner, Elisa, Sicherheit am Bahnhof – Überwachungsmaßnahmen zur Abwehr terroristischer Anschläge, Berlin 2017.

Stokes, Elaisha, Wrongful arrest exposes racial bias in facial recognition technology, CBS News v. 19.11.2020, abrufbar unter https://www.cbsnews.com/news/detroit-facial-recognition-surveillance-camera-racial-bias-crime/ [https://perma.cc/AM59-9P7P].

Strauss, Anselm L. / Corbin, Juliet M., Grounded Theory: Grundlagen Qualitativer Sozialforschung, Weinheim 1996.

Summary report of the project "Towards the European Level Exchange of Facial Images" (TELEFI) 2021, abrufbar unter https://www.telefi-project.eu/sites/default/files/TELEFI_SummaryReport.pdf [https://perma.cc/T6NE-GTRV].

Sydow, Gernot / Marsch, Nikolaus (Hrsg.), Datenschutz-Grundverordnung Bundesdatenschutzgesetz Handkommentar, 3. Aufl., Baden-Baden 2022 (zitiert als: Sydow/Marsch DS-GVO/BDSG/*Bearbeiter*).

Szymanski, Mike, Spähangriff mit 17.000 Kameras, Süddeutsche Zeitung v. 27.2.2013, abrufbar unter https://www.sueddeutsche.de/bayern/videoueberwachung-in-bayern-spaeh-angriff-mit-17-000-kameras-1.1610655 [https://perma.cc/2A3R-2V7T].

Taeger, Jürgen / Gabel, Detlev (Hrsg.), DSGVO - BDSG – TTDSG, 4. Aufl., Frankfurt am Main 2022 (zitiert als: Taeger/Gabel/*Bearbeiter*).

Taigman, Yaniv / Yang, Ming / Ranzato, Marc'Aurelio / Wolf, Lior, DeepFace: Closing the Gap to Human-Level Performance in Face Verification, Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition 2014, 1701-1708.

Tan, Zichang / Guo, Guodong, Face Recognition Research and Development, in: Li, Stan Z. / Jain, Anil K. / Deng, Jiankang (Hrsg.), Handbook of Face Recognition, 3. Aufl., Cham 2024, 3-36.

Tanneberger, Steffen, Die Sicherheitsverfassung – Eine systematische Darstellung der Rechtsprechung des Bundesverfassungsgerichts. Zugleich ein Beitrag zu einer induktiven Methodenlehre, Tübingen 2014.

Thanawala, Sudhin, Facial Recognition Technology Jailed a Man for Days, AP News v. 25.9.2023, abrufbar unter https://apnews.com/article/mistaken-arrests-facial-recognition-technology-lawsuits-b613161c56472459df683f54320d08a7 [https://perma.cc/6PU3-PB8F].

Thiel, Markus, Die Vermessung der Welt? – Zur Nutzung biometrischer Identifikationssysteme durch die Sicherheitsbehörden, ZRP 2016, 218-221.

Tischbirek, Alexander / Wihl, Tim, Verfassungswidrigkeit des Racial Profiling, JZ 2013, 219-224.

Tistarelli, Massimo / Champod, Christophe, Biometric Technologies for Forensic Science and Policing: State of the Art, in: Tistarelli, Massimo / Champod, Christophe (Hrsg.), Handbook of Biometrics for Forensic Science, Cham 2017, 1-15.

Töpfer, Eric, Videoüberwachung als Kriminalprävention? – Plädoyer für einen Blickwechsel, Kriminologisches Journal 2009, 272-281.

Tomaszewska-Michalak, Magdalena, Biometric Technology 20 Years After 9/11 – Opportunities and Threats, Studia Politologiczne 2022, 123-134.

Tomerius, Carolyn, „Drohnen" zur Gefahrenabwehr – Darf die Berliner Polizei nach jetziger Rechtslage Drohnen präventiv-polizeilich nutzen?, LKV 2020, 481-489.

Trute, Hans-Heinrich, Grenzen des präventionsorientierten Polizeirechts in der Rechtsprechung des Bundesverfassungsgerichts, Die Verwaltung 2009, 85-104.

Tschorr, Sophie, Regulierung der auf Biometrie basierenden KI-Systeme, MMR 2024, 304-307.

Turk, Matthew A. / Pentland, Alex P., Eigenfaces for Recognition. Journal of Cognitive Neuroscience 1991, 71–86.

Turk, Matthew A. / Pentland, Alex P., Face recognition using eigenfaces, Proceedings of the IEEE Computer Science Conference on Computer Vision and Pattern Recognition 1991, 586-591.

Uhl, Andreas, State of the Art in Vascular Biometrics, in: Uhl, Andreas / Busch, Christoph / Marcel, Sébastien / Veldhuis, Raxmond (Hrsg.), Handbook of Vascular Biometrics, Cham 2020, 3-62.

Ungern-Sternberg, Antje v., Discriminatory AI and the Law: Legal Standards for Algorithmic Profiling, in: Vöneky, Silja / Kellmeyer, Philipp / Müller, Oliver / Burgard, Wolfram (Hrsg.), The Cambridge Handbook of Responsible Artificial Intelligence, 2022, 252-280.

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.

Valentino-DeVries, Jennifer, How the Police Use Facial Recognition, and Where It Falls Short, The New York Times v. 12.1.2020, abrufbar unter https://www.nytimes.com/2020/01/12/technology/facial-recognition-police.html [https://perma.cc/M7LL-DY24].

Valta, Matthias/Vasel, Justus, Kommissionsvorschlag für eine Verordnung über Künstliche Intelligenz, ZRP 2021, 142-145.

van Heek, Julia / Arning, Katrin / Ziefle, Martina, The Surveillance Society: Which Factors Form Public Acceptance of Surveillance Technologies?, in: Helfert, Markus / Klein, Cornel / Donnelley, Brian / Gusikhin, Oleg (Hrsg.), Smart Cities, Green Technologies, and Intelligent Transport Systems, Cham 2017, 170-191.

van Oorschot, Frederike / Fucker, Selina (Hrsg.), Framing KI – Narrative, Metaphern und Frames in Debatten über Künstliche Intelligenz, Heidelberg 2022.

Vasel, Johann Justus / Heck, Annika Pia, KI-basierte Assistenzsysteme im Asylverfahren und ihre Verfassungskonformität, NVwZ 2024, 540-547.

von Lewinski, Kai, Die Matrix des Datenschutzes – Besichtigung und Ordnung eines Begriffsfeldes, Heidelberg 2014.

Voßkuhle, Andreas / Schemmel, Jakob, Grundwissen – Öffentliches Recht: Die Versammlungsfreiheit, JuS 2022, 1113-1117.

Wachter, Sandra / Mittelstadt, Brent / Russell, Chris, Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI, Computer Law & Security Review 2021, 1-72.

Wahl, Rainer / Masing, Johannes, JZ 1990, 553-563.

Walburg, Christian, Kriminell oder kriminalisiert? Die Rolle der Polizei bei Verdachtsschöpfung und Konstruktion der „Ausländerkriminalität, in: Hunold, Daniela / Singelnstein, Tobias (Hrsg.), Rassismus in der Polizei. Eine wissenschaftliche Bestandsaufnahme, Wiesbaden 2022, 385-404.

Watkins, Ali, How the N.Y.P.D. Is Using Post-9/11 Tools on Everyday New Yorkers, The New York Times v. 8.9.2021, abrufbar unter https://www.nytimes.com/2021/09/08/nyregion/nypd-9-11-police-surveillance.html [https://perma.cc/LB56-EABB].

Weber, Frank, Gesichtserkennung, in: Behrens, Michael / Roth, Richard (Hrsg.), Biometrische Identifikation. Grundlagen, Verfahren, Perspektiven, Braunschweig 2001, 105-128.

Wehrheim, Jan, Definitionsmacht und Selektivität in Zeiten neuer Kontrolltechnologien, in: Schmidt-Semisch, Henning / Hess, Henner, Die Sinnprovinz der Kriminalität. Zur Dynamik eines sozialen Feldes, Wiesbaden 2014, 137-153.

Wei, Xingjie / Li, Chang-Tsun, Face Recognition Technologies for Evidential Evaluation of Video Traces, in: Tistarelli, Massimo / Champod, Christophe (Hrsg.), Handbook of Biometrics for Forensic Science, Cham 2017, 177-193.

Wells, Gary L. / Kovera, Margaret B. / Douglass, Amy B. / Brewer, Neil / Meissner, Christian A. / Wixted, John T., Policy and Procedure Recommendations for the Collection and Preservation of Eyewitness Identification Evidence, Law and Human Behavior 2020, 3-36.

Wendehorst, Christiane / Nessler, Bernhard / Aufreiter, Alexander / Aichinger, Gregor, Der Begriff des „KI-Systems" unter der neuen KI-VO, MMR 2024, 605-614.

Wendel, Matthias, Das Bundesverfassungsgericht als Garant der Unionsgrundrechte – Zugleich Besprechung von BVerfG, Beschlüsse v. 6. 11. 2019–1 BvR 16/13 (Recht auf Vergessen I) und 1 BvR 276/17 (Recht auf Vergessen II), JZ 2020, 157-168.

Werner, G., Dritte Dimension des Erkennungsdienstes, Bayerns Polizei 2017, Heft 4, 24

White, David / Dunn, James D. / Schmid, Alexandra C. / Kemp, Richard I., Error Rates in Users of Automatic Face Recognition Software, PLOS One 2015, 1-14.

Wilding, Mark, IBM promised to back off facial recognition – then it signed a $69.8 million contract to provide it, The Verge v. 31.8.2023, abrufbar unter https://www.theverge.com/2023/8/31/23852955/ibm-uk-government-contract-biometric-facial-recognition [https://perma.cc/Q533-Z8AV].

Wimmer, Susi, Selfies könnten in Zukunft Verbrechen aufklären, Süddeutsche Zeitung v. 16.1.2016, abrufbar unter https://www.sueddeutsche.de/muenchen/gesichtserkennung-bei-der-polizei-selfies-koennten-in-zukunft-verbrechen-aufklaeren-1.2820125 [https://perma.cc/5AWG-M9DZ].

Wintrich, Josef M., Zur Problematik der Grundrechte, Köln/Opladen 1957.

Wittmann, Philipp, Nobody Watches the Watchmen – Rechtliche Rahmenbedingungen und zunehmende Ausweitung der öffentlichen Videoüberwachung in den USA, ZaöRV 2013, 373-426.

Wörner, Liane / Blocher, Janine, German report on criminalisation of AI-related offences (AIDP Landesbericht, Sektion II Strafrecht Besonderer Teil), in: Miró-Llinares, Fernando / Duvac, Constantin / Toader, Tudorel / Santisteban Galazarza, Mario (Hrsg.), Criminalisation of AI-related offences, International Colloquium, Bucharest, Romania, 14-16 June 2023, RIDP (1) 2024, 213-244.

Wolff, Heinrich Amadeus / Brink, Stefan / Ungern-Sternberg, Antje v. (Hrsg.), Beck'scher Online-Kommentar Datenschutzrecht, 46. Ed., Stand: 1.8.2023 / 1.11.2023, München 2023 (zitiert als: BeckOK DatenschutzR/*Bearbeiter*).

Wolter, Jürgen, Heimliche und automatisierte Informationseingriffe wider Datengrundrechtsschutz – Gesamtanpassung vor Gesamtreform von Strafprozeß- und Polizeirecht, (2. Teil), GA 1988, 129-142.

Wolter, Jürgen (Hrsg.), Systematischer Kommentar zur Strafprozessordnung: SK-StPO, Band II: §§ 94-136a StPO, 6. Aufl., München 2023 (zitiert als: SK-StPO/*Bearbeiter*).

Yadav, Daksha / Kohli, Naman / Pandey, Prateekshit / Singh, Richa / Vatsa, Mayank / Noore, Afzel, Effect of illicit drug abuse on face recognition, Proceedings of the IEEE Winter Conference on Applications of Computer Vision 2016, 1-7.

Zöller, Mark A. / Ihwas, Saleh, Rechtliche Rahmenbedingungen des polizeilichen Flugdrohneneinsatzes, NVwZ 2014, 408-414.

Zöller, Mark A., Informationssysteme und Vorfeldmaßnahmen von Polizei, Staatsanwaltschaft und Nachrichtendiensten – Zur Vernetzung von Strafverfolgung und Kriminalitätsverhütung im Zeitalter von multimedialer Kommunikation und Persönlichkeitsschutz, Heidelberg 2002.

Zöller, Mark A., Möglichkeiten und Grenzen polizeilicher Videoüberwachung, NVwZ 2005, 1235-1241.

Zweig, Katharina A. / Krafft, Tobias D., Fairness und Qualität algorithmischer Entscheidungen, in: Mohabbat Kar, Resa / Thapa, Basanta / Parycek, Peter (Hrsg.), (Un)Berechenbar? Algorithmen und Automatisierung in Staat und Gesellschaft, 2018, 204-227.