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.

I. 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, 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.