Kapitel I. Grundlagen

„Daten sind Macht."[1]

A. Einführung

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

B. Ziel und Gang der Untersuchung

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

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

---

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

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

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

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

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

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

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

C. Gesichtserkennung in der Strafverfolgung: Abgrenzung und Einsatzszenarien

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

I. Abgrenzung

1. Andere Methoden der biometrischen Erkennung

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

13 Ausführlich zum technologischen Hintergrund Kapitel I. E.

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

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

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

2. Andere Formen der Gesichtsanalyse

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

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

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

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

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

3. Andere Einsatzbereiche

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

II. Einsatzszenarien in der Strafverfolgung

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

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

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

1. Identitätsermittlung

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

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

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

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

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

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

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

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

2. Auswertung von umfangreichem Datenmaterial

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

30 *Hill*, The New York Times v. 18.1.2020, https://perma.cc/C4H9-NC6H.
31 Vgl. auch *Schindler*, Biometrische Videoüberwachung, 2021, 191.
32 Siehe etwa für die EU-Staaten Summary report of the project „Towards the European Level Exchange of Facial Images" (TELEFI), 2021, 10 ff., https://perma.cc/T6NE-GTRV.
33 Näher beschrieben bei VG Hamburg Urt. v. 23.10.2019, 17 K 203/19, BeckRS 2019, 40195 Rn. 1 ff.; kritisch zu der Entscheidung *Mysegades*, NVwZ 2020, 852.
34 VG Hamburg, Urt. v. 23.10.2019, 17 K 203/19, BeckRS 2019, 40195 Rn. 3.
35 So noch die Formulierung in VG Hamburg, Urt. v. 23.10.2019, 17 K 203/19, BeckRS 2019, 40195 Rn. 4; mittlerweile ist in der computerwissenschaftlichen Literatur der Begriff „Embedding" geläufiger.

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

3. Digitale Beobachtung

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

---

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

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

38 Dies gilt nicht nur für Bilder, bei denen der Ort sichtbar ist, sondern grundsätzlich für alle digitalen Fotos, da sie zusätzliche Informationen enthalten (sog. Exif-Daten), z. B. über den Ort und die Zeit ihrer Aufnahme.

4. Echtzeit-Fahndung

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

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

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

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

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

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

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

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

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

D. Forschungszuschnitt dieser Arbeit

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

I. Besonderes Gefährdungspotenzial der Gesichtserkennung

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

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

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

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

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

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

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

1. Streubreite

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

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

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

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

2. Fehleranfälligkeit

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

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

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

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

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

3. Heimlichkeit

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

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

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

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

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

4. Vernetzungsmöglichkeit

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

5. Biometrie

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

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

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

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

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

6. Fazit

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

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

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

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

II. Relevantestes Einsatzszenario: Identitätsermittlung

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

III. Stand der Forschung und Forschungslücke

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

64 Hierzu Kapitel I. F.

65 Kapitel I. G. II.

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

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

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

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

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

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

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

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

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

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

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

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

IV. Notwendigkeit einer Regulierung

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

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

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

76 BT-Drs. 20/5781, 8.

77 Kapitel I. F. II.

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

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

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

E. Technologie

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

I. Verifizierung vs. Identifizierung

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

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

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

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

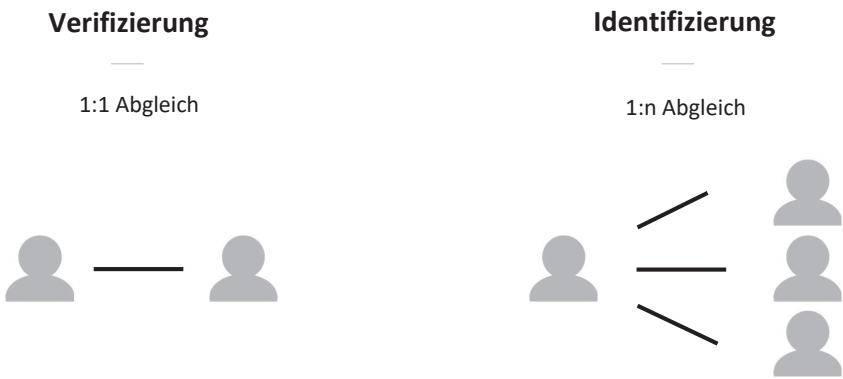

Abbildung 1: Verifizierung vs. Identifizierung

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

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

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

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

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

II. Entwicklung der automatisierten Gesichtserkennung

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

1. Anfänge der Forschung

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2. Nutzbarmachung für die Strafverfolgung

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

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

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

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

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

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

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

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

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

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

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

3. Durchbruch durch große Datenbestände und maschinelles Lernen

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

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

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

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

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

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

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

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

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

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

4. Neue Akteure

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

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

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

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

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

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

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

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

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

III. Ablauf einer Erkennung

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

119 *Hill*, The New York Times v. 18.1.2020, https://perma.cc/C4H9-NC6H.
120 Vgl. die Webseite von *Clearview AI*, How We Store and Search 30 Billion Faces, https://perma.cc/26PG-KURE.
121 *Clayton/Derico*, BBC v. 27.3.2023, https://perma.cc/Q97Q-YFPQ.
122 *Hill*, Your Face Belongs to Us, 249 f. Über China wird berichtet, dass die Polizei an einigen Orten bereits 2018 Sonnenbrillen mit integrierter Gesichtserkennung nutzte, *Mozur*, The New York Times v. 8.7.2018, https://perma.cc/BC7A-GUN5.
123 *Hill*, Your Face Belongs to Us, 249 f.
124 *Bledsoe*, „I Had a Dream: AAAI Presidential Address", 19 August 1985, AI Magazine 1986, 57, 61.
125 Der Begriff Template wird ebenfalls gebraucht, neuere Publikationen verwenden hingegen überwiegend den Begriff Embeddings.

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

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

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

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

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

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

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

131 Ausführlich zu den Fehlerraten von Gesichtserkennung sogleich unter III.

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

IV. Fehlerraten

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

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

1. Arten von Fehlern

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

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

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

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

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

a) Falsche Nichttreffer (False negatives)

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

b) Falsche Treffer (False positives)

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

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

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

c) Messung

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

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

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

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

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

2. Ursachen von Fehlern

a) Unterschiedliche Leistungsfähigkeit verschiedener Systeme

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

b) Unkooperatives Setting

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

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

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

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

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

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

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

c) Qualität der abzugleichenden Bilder

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

d) Alterung und Gesichtsabnutzung

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

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

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

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

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

e) Größe der Datenbank

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

f) Gewählter Schwellenwert

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

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

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

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

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

3. „Erwünschte" Fehler

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

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

---

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

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

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

4. Stand der Technik

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

a) Ergebnisse der Face Recognition Vendor Tests des NIST

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

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

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

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

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

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

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

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

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

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

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

b) Einordnung

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

5. Höhere Fehlerraten bei einigen Bevölkerungsgruppen

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

173 Vgl. nur *Niemz/Singelnstein*, in: Hunold/Singelnstein, Rassismus in der Polizei, 2022, 337; *Abdul-Rahman*, in: Hunold/Singelnstein Rassismus in der Polizei, 2022, 471, 479 mwN; *Hunold/Wegner*, Aus Politik und Zeitgeschichte 2020, 27, 30 f.; *Hunold*, Polizei im Revier, 2015, 103 ff.; *Schweer/Strasser/Zdun*, „Das da draußen ist ein Zoo, und wir sind die Dompteure" – Polizisten im Konflikt mit ethnischen Minderheiten und sozialen Randgruppen, 2008; *Schweer/Strasser*, in: Groenemeyer/Mansel, Die Ethnisierung von Alltagskonflikten, 2003, 229. Zu häufigeren Kontrollen und Festnahmen Schwarzer und Hispanics in den USA, selbst bei geringfügigen Vergehen, siehe *Heath*, USA TODAY v. 19.11.2014, https://perma.cc/5YQ8-T6WM; mit Blick auf stop-and-frisks *Goel/Rao/Shroff*, Annals of Applied Statistics, 2016, 365, 367 („[W]e find that blacks and Hispanics were disproportionately involved in low hit rate stops."); *Gelman/Fagan/Kiss*, Journal of the American Statistical Association 2007, 813, 821 („In the period for which we had data, the NYPD's records indicate that they were stopping blacks and Hispanics more often than whites, in comparison to both the populations of these groups and the best estimates of the rate of crimes committed by each group.").

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

6. Fazit

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

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

F. Einsatz in Deutschland

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

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

I. Gesichtserkennungssystem GES beim BKA

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

1. Durchsuchbare Datenbank: INPOL-Z

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

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

176 BT-Drs. 20/895, 9.

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

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

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

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

181 BT-Drs. 20/895, 9.

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

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

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

---

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

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

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

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

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

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

2. Ablauf

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

a) Bild eines Tatverdächtigen

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

189 BT-Drs. 20/895, 9.

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

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

192 BT-Drs. 20/5781, 8.

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

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

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

b) Generierung einer Kandidatenliste

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

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

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

c) Überprüfung durch Experten

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

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

---

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

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

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

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

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

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

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

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

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

d) Weitere Ermittlungsmaßnahmen

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

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

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

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

e) Case Study einer Recherche im GES

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

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

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

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

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

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

en Aufnahmen aus erkennungsdienstlichen Behandlungen weitergeblättert werden.

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

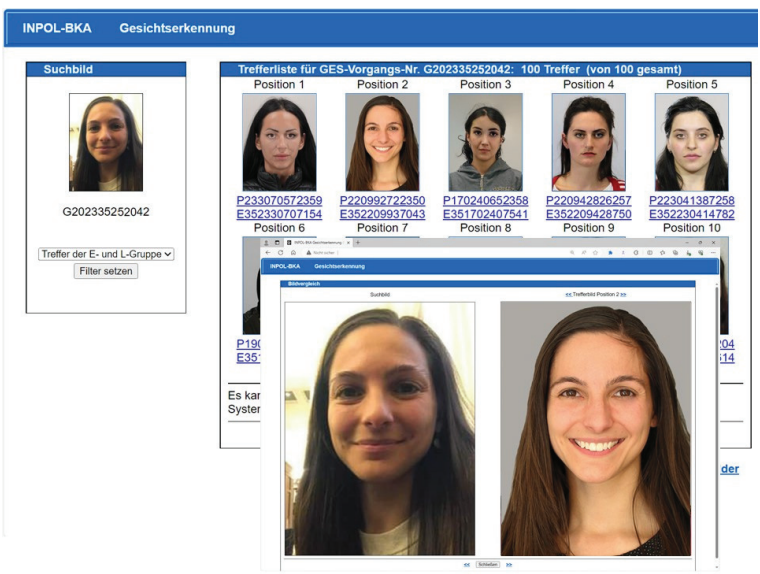

Abbildung 3: Fiktives Beispiel einer Recherche im GES

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

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

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

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

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

3. Keine näheren Informationen über Trainingsprozess des GES

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

4. Keine Evaluierung der grundsätzlichen Leistungsfähigkeit des GES

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

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

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

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

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

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

5. Keine Evaluierung der auf GES-Recherchen basierenden Ermittlungsverfahren

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

II. Landeskriminalämter und Landespolizeibehörden

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

1. Schnittstellen zum GES bei den Landeskriminalämtern

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

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

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

2. Eigene Systeme beim LKA Bayern und anderen Landespolizeibehörden

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

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

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

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

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

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

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

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

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

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

III. Einordnung

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

---

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

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

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

G. Chancen und Risiken des Einsatzes

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

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

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

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

I. Potenzial für die Strafverfolgung

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

---

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

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

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

1. Effizienz

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

2. Einfache Erfassung und Verfügbarkeit von Gesichtsbildern

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

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

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

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

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

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

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

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

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

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

242 Wie bereits erwähnt, befindet sich die Retina (Netzhaut) am hinteren Teil des Auges und kann nur aus der Entfernung weniger Zentimeter gescannt werden; die Person muss zudem ihren Kopf für etwa 10–30 Sekunden stillhalten (zur Retina-Erkennung siehe nur *Uhl*, in: Uhl/Busch/Marcel/Veldhuis, Handbook of Vascular Biometrics, 2020, 3, 8 f.; *Semerád/Drahanský*, in: Uhl/Busch/Marcel/Veldhuis, Handbook of Vascular Biometrics, 2020, 309, 313). Iriserkennungen waren ursprünglich nur aus einer Entfernung von weniger als einem Meter und mit Kooperation des Betroffenen zuverlässig möglich. Zwar wird in den letzten Jahren vermehrt daran geforscht, eine höhere Genauigkeit zu erreichen, auch für die Erkennung aus mehreren Metern Entfernung und/oder in nicht kontrollierten Settings (unconstrained environments), bei denen die Betroffenen sich bewegen oder nicht direkt in die Kamera blicken, siehe nur *Nguyen/Fookes/Jillela/Sridharan/Ross*, Pattern Recognition 2017, 123; *Tistarelli/Champod*, in: Tistarelli/Champod, Handbook of Biometrics for Forensic Science, 2017, 1, 4. Die Genauigkeit solcher Iriserkennungen liegt dennoch weit hinter denen einer Gesichtserkennung.

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

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

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

3. Gesichtserkennung als einziger Spurenansatz

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

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

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

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

4. Überprüfbarkeit durch Menschen

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

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

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

250 Kapitel I. E. III.

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

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

II. Risiken

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

1. Erfahrung aus anderen Staaten

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

a) USA

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

b) China

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

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

c) Russland

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

Näheres darüber, wie solche Festnahmen ablaufen können, wurde anlässlich eines EGMR-Urteils[280] gegen Russland im Jahr 2023 bekannt. Der Beschwerdeführer war mit der Moskauer U-Bahn gefahren und trug dabei eine lebensgroße Pappfigur des inhaftierten Kreml-Kritikers Konstantin Kotov mit sich, der ein Schild in Händen hatte mit der Aufschrift „А вы не о*уели? Я Константин Котов, за мирные пикеты мне грозит до 5 лет." („Seid ihr bescheuert? Ich bin Konstantin Kotov, mir drohen bis zu 5 Jahre wegen friedlichen Protests.").[281] Von der Protestaktion wurden Fotos

274 Vgl. auch *Kuteynikov/Izhaev/Lebedev/Zenin*, Lex Russica 2022, 121, 127.
275 EGMR, Urt. v. 4.7.2023, 11519/20, Rn. 5.
276 *Kuteynikov/Izhaev/Lebedev/Zenin*, Lex Russica 2022, 121, 127.
277 So die russische Nichtregierungsorganisation OVD-Info, 17.1.2022, https://perma.cc/A57N-KBET.
278 *Solopov*, Meduza v. 27.4.2021, https://perma.cc/KD8C-BCGJ.
279 *Masri*, Reuters v. 28.3.2023, https://perma.cc/L7QD-B5UA.
280 EGMR, Urt. v. 4.7.2023, 11519/20. Russland ist zwar seit 16.9.2022 nicht mehr Vertragspartei der EMRK, für die Bearbeitung der bis zu diesem Zeitpunkt eingereichten Beschwerden gegen Russland ist der EGMR aber weiterhin zuständig, vgl. Art. 58 Abs. 2 EMRK.
281 Hierzu die russische Nichtregierungsorganisation OVD-Info, 4.7.2023, https://perma.cc/LTU2-X85U; in der Entscheidung des EGMR findet sich die Formulierung

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

2. Zentrale Probleme

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

„You must be f**king kidding me. I'm Konstantin Kotov. I'm facing up to five years [in prison] under [Article] 212.1 for peaceful protests.", EGMR, Urt. v. 4.7.2023, 11519/20 Rn. 7.

282 Dass die Polizei Gesichtserkennung eingesetzt hatte, gaben die Regierungsvertreter Russlands zwar während des Verfahrens vor dem EGMR nicht ausdrücklich zu. Die Richterinnen und Richter sahen die Verwendung aber als erwiesen an, weil nicht erklärbar war, wie die Polizei den Demonstranten so schnell nach seinem Protest identifizieren konnte, EGMR, Urt. v. 4.7.2023, 11519/20 Rn. 72. Da die russische Polizei den Einsatz von Gesichtserkennung nicht dokumentieren und Betroffene auch nicht darüber informieren muss, sei es im Übrigen für die Bürger kaum möglich, den Einsatz zu beweisen.

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

a) Fehlidentifizierung und Ermittlungsmaßnahmen gegen Unbeteiligte

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

b) Privatheit der Betroffenen

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

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

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

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

c) Auswirkungen auf die gesamte Gesellschaft

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

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

3. Relevanz für Deutschland

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

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

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

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

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

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

290 § 147 Abs. 4 StPO.

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

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

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

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

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

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

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

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

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

298 BVerfG, NJW 2023, 3698, 3708.

H. Fazit zu Kapitel I. Grundlagen

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