Kapitel IV. Empfehlungen für eine Regulierung

In diesem Kapitel soll aus den vorangegangenen Erkenntnissen ein konkreter Vorschlag für eine Regulierung des Einsatzes automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger erarbeitet werden. Dieser Vorschlag und die Empfehlungen erheben nicht den Anspruch, vollumfänglich zu sein, sondern sollen den Ausgangspunkt für eine weitere Diskussion in der Rechtswissenschaft und Kriminologie bilden. Besonders wertvoll wäre, hierzu in Zukunft auch in Austausch mit anderen Disziplinen wie der Informatik und der Soziologie zu treten. Insbesondere sollten diese Vorschläge lediglich als Mindestvorgaben verstanden werden; die Frage, inwieweit der Einsatz automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger zugelassen werden soll, bedarf eines rechtspolitischen Diskurses der Öffentlichkeit.

Im Folgenden wird zunächst auf die technischen Anforderungen an Gesichtserkennungssysteme eingegangen (A.), dann werden die Vorgaben für eine Rechtsgrundlage und ein Formulierungsvorschlag erarbeitet (B.) und schließlich weitere Empfehlungen, insbesondere zu Evaluation, Kontrolle und Berichtspflichten, vorgestellt (C.).

A. Technische Anforderungen an die verwendeten Gesichtserkennungssysteme

I. Genauigkeit und Freiheit von demografischen Verzerrungen

Die verwendeten Gesichtserkennungssysteme müssen dem jeweils aktuellen Stand der Technik entsprechen und daran gemessen ein Höchstmaß an Genauigkeit erfüllen.[1057] Näher ausformulierte Vorgaben, etwa zu den Fehlerraten, sind wegen des schnellen technologischen Fortschritts nicht ratsam. Festgelegt werden sollte zudem, dass die Systeme von einer unab-

1057 Vgl. auch *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, 2023, 506, 772 zu einer ähnlichen Formulierung für Regelungen zum Einsatz von statistischen und selbstlernenden Data Mining-Methoden im Strafverfahren.

hängigen Stelle wie dem NIST[1058], nicht etwa nur von dem Anbieter selbst, evaluiert sein müssen. Zwar ist tendenziell bei den genauesten Gesichtserkennungssystemen zu erwarten, dass sie auch vergleichbare Fehlerraten für unterschiedliche Bevölkerungsgruppen aufweisen;[1059] auf solche Erfahrungswerte sollte beim Einsatz von Gesichtserkennung in einem sensiblen Bereich wie der Strafverfolgung aber nicht abgestellt werden. Stattdessen sollten die eingesetzten Gesichtserkennungssysteme vor ihrem Einsatz von einer unabhängigen Stelle wie beispielsweise dem NIST zusätzlich auch auf demografische Verzerrungen hin untersucht worden sein. Auch wenn die Fehlerraten für verschiedene Bevölkerungsgruppen nicht exakt gleich ausfallen werden, sollten sie sich jedoch in einem vergleichbaren Rahmen bewegen.

II. Einrichtung einer zentralen Zertifizierungsstelle

Um sicherzustellen, dass diese Anforderungen erfüllt sind, ist eine zentrale Zertifizierungsstelle für in der Strafverfolgung verwendete Gesichtserkennungssysteme einzurichten. Diese testet die Systeme nicht selbst,[1060] sondern prüft anhand der Ergebnisse der externen Evaluation, ob das System dem aktuellen Stand der Technik entspricht. Hierüber wird ein Zertifikat ausgestellt. Die Rechtsgrundlage für den Einsatz automatisierter Gesichtserkennung sollte dann festlegen, dass nur von dieser Stelle zertifizierte Gesichtserkennungssysteme eingesetzt werden dürfen. Zudem sollte die Exekutive ermächtigt werden, durch Rechtsverordnung eine solche Stelle zu errichten und das nähere Verfahren (z. B. Dauer der Gültigkeit der Zertifikate) zu regeln.[1061] Ein solcher Regulierungsansatz würde gewährleisten, dass – anders als gegenwärtig der Fall – jede Polizeibehörde, die ein Gesichtserkennungssystem anschafft, dieses zunächst unabhängig evaluie-

1058 Zum NIST Kapitel I. E. IV. 4.

1059 Kapitel I. E. IV. 5.

1060 Hierfür wäre ein großer Ressourcenaufwand (insbesondere eine Testdatenbank und Fachkräfte) nötig, der angesichts der bereits bestehenden verlässlichen und renommierten unabhängigen Bewertungsstellen wie dem NIST nicht sinnvoll erscheint.

1061 Vgl. auch den Vorschlag von *Rückert*, Digitale Daten als Beweismittel im Strafverfahren, 2023, 772 für die Einrichtung von Stellen zur Zertifizierung von Blackbox-Programmen, die zum Data Mining eingesetzt werden.

ren lassen[1062] und dann eine Zertifizierung beantragen muss. So kommen nur Systeme zur Anwendung, die dem Stand der Technik entsprechen. Dies kann angesichts der Bedenken in der Bevölkerung hinsichtlich Fehleranfälligkeit und Diskriminierung durch Gesichtserkennungssysteme[1063] auch dazu beitragen, das Vertrauen in die polizeiliche Arbeit mit neuen Strafverfolgungstechnologien zu erhöhen.

Unter Umständen könnte sich eine solche zentrale Zertifizierungsstelle in Zukunft durch das Konformitätsbewertungsverfahren[1064] nach Art. 43 KI-VO für Hochrisiko-KI-Systeme (also auch für biometrische Fernidentifizierungssysteme wie automatisierte Gesichtserkennung) erübrigen. Dann müsste dieses geeignet sein, sicherzustellen, dass nur Gesichtserkennungssysteme zur Anwendung kommen, die dem aktuellen Stand der Technik entsprechen und daran gemessen ein Höchstmaß an Genauigkeit erfüllen. Derzeit ist dies aber nicht gesichert, denn Art. 15 Abs. 1 KI-VO fordert lediglich ein „angemessenes" Maß an Genauigkeit. Dieser Maßstab soll zukünftig durch Normierungsinstitutionen näher konkretisiert werden. Dies ist nicht unkritisch zu sehen, denn damit gehen regelmäßig auch Wertentscheidungen mit einher.[1065] Gerade für den besonders sensiblen Bereich der Strafverfolgung sollten solche Wertentscheidungen wohlüberlegt, mit äußerster Sorgfalt und unter Berücksichtigung der Konsequenzen für die Betroffenen getroffen werden. Derzeit ist noch nicht abzusehen, ob dies mit den Vorgaben der KI-Verordnung gewährleistet werden kann. Auch wenn der hier unterbreitete Vorschlag einer nationalen Zertifizierungsstelle für Gesichtserkennungssysteme eine weitere Vorgabe für den Einsatz von Gesichtserkennungstechnologie und damit weitere bürokratische Hürden schafft: Solange nicht sichergestellt ist, dass die KI-Verordnung so ausgelegt und konkretisiert wird, dass nur Systeme zur Anwendung kommen, die dem Stand der Technik entsprechen, sollte dies durch eine nationale Zertifizierungsstelle abgesichert werden.[1066]

1062 Oder die Polizei müsste bereits evaluierte Systeme erwerben.

1063 *Kostka/Steinacker/Meckel*, Public Understanding of Science 2021, 671, 683 f.; zur Darstellung von Gesichtserkennung als „rassistische Technologie" Kapitel III. C. III. 2. b) cc) und Kapitel III. C. IV. 2.

1064 Hierzu Kapitel II. B. I. 1. b) aa).

1065 Kritisch auch *Martini*, in: Martini/Wendehorst, KI-VO, Art. 15 Rn. 37; vgl. auch *Guijarro Santos*, ZfDR 2023, 23, 33 f.

1066 Selbstverständlich ließe sich einwenden: Wird dieser Zertifizierungsstelle damit nicht ebenfalls eine Wertentscheidung überlassen? Das ist zutreffend, allerdings wird dieser (notwendige) Umstand durch zwei Faktoren abgemildert: Erstens wird

B. Rechtsgrundlage

I. Vorgaben des Grundsatzes der Bestimmtheit und Normenklarheit

Um dem Grundsatz der Bestimmtheit und Normenklarheit sowie dem Wesentlichkeitsprinzip zu genügen, muss die Rechtsgrundlage zumindest den konkreten Zweck der Maßnahme erkennen lassen, die zum Abgleich zugelassenen Datenbanken beschreiben und begrenzen, das technische Eingriffsinstrument benennen und die Verwendung biometrischer Merkmale offenlegen.

1. Formulierung des Zwecks

Der Zweck der Maßnahme, also die Identifizierung unbekannter Verdächtiger, muss konkret benannt werden.[1067] Eine offene Formulierung wie in § 98c StPO („zur Aufklärung einer Straftat") mag für geringfügige Grundrechtseingriffe ausreichend sein, bei erheblichen Eingriffen wie der Gesichtserkennung muss das Gesetz die Zielrichtung der Maßnahme näher erkennen lassen. Dabei ist eine möglichst genaue Beschreibung wie „zur Identifizierung unbekannter Verdächtiger" zu empfehlen. Zugleich würde dadurch sichergestellt, dass sich die Maßnahmen nur gegen den Beschuldigten, nicht etwa – wie dies bei § 98c StPO möglich ist – gegen Zeugen richten dürfen.

2. Begrenzung der Datenbanken

Der Gesetzgeber muss zudem die zum Abgleich zugelassenen Datenbanken klar benennen und dadurch wirksam begrenzen.[1068] Besonders kritisch

---

in dieser Arbeit vorgeschlagen, dass die Systeme nicht nur ein „angemessenes" Maß, sondern ein Höchstmaß an Genauigkeit aufweisen müssen. Zweitens könnte die in dieser Arbeit ebenfalls vorgeschlagene – siehe unten – noch einzusetzende interdisziplinär besetzte Evaluationskommission von Gesichtserkennungssystemen die Entscheidungen der Zertifizierungsstelle kritisch hinterfragen und so einen Diskurs anstoßen; dessen Ergebnisse könnten dann auch realistisch zeitnah (anders als bei Normierungsinstituten auf EU-Ebene) in Deutschland umgesetzt werden.

1067 Kapitel II. A. I. 3. b) und Kapitel II. C. I. 2. a).

1068 Kapitel II. A. I. 3. b) und Kapitel II. C. I. 2. c).

sollte hinterfragt werden, ob pauschal bei jeder Gesichtserkennungssuche – wie derzeit mit dem BKA-GES praktiziert –[1069] ein Abgleich mit den Lichtbildern aller Asylsuchenden zulässig sein kann. Solche grundlegenden Fragen zur Streubreite der Maßnahme und damit zur Anzahl der Grundrechtseingriffe muss im Rahmen eines demokratischen Prozesses entschieden werden. Bei Erlass der Rechtsgrundlage für eine neue Datenbank muss der Gesetzgeber dann stets auch neu entscheiden, ob diese per Gesichtserkennung durchsucht werden darf, um unbekannte Verdächtige zu identifizieren.

3. Benennung des technischen Eingriffsinstruments

Weiterhin ist in der Rechtsgrundlage das technische Eingriffsinstrument – die automatisierte Gesichtserkennung – eindeutig zu benennen.[1070] Die Vorschrift des Art. 61 Abs. 2 BayPAG, die insbesondere den Einsatz von Gesichtserkennungssoftware erlauben soll,[1071] sieht beispielsweise vor, dass der Abgleich personenbezogener Daten „auch unter Verwendung bildverarbeitender Systeme und durch Auswertung biometrischer Daten erfolgen" kann. Eine solch offene Beschreibung des technischen Eingriffsinstruments erscheint im sensiblen Bereich der Verarbeitung biometrischer Daten zu unbestimmt. Unter die Formulierung würden sich nicht nur Gesichtserkennungssysteme, sondern auch andere biometrische Identifizierungssysteme[1072] und sogar Emotionserkennungssysteme[1073] subsumieren lassen; diese bedürfen jedoch einer anderen verfassungsrechtlichen und kriminalpolitischen Betrachtung sowie anderer Schutzvorkehrungen als die Gesichtserkennung. Eine Rechtsgrundlage für den Einsatz von Gesichtserkennung sollte dieses technische Eingriffsinstrument ausdrücklich benennen. So lässt die Vorschrift die zugelassene Maßnahme für den Rechtsanwender und Betroffene erkennen und begrenzt zugleich das Eingriffsinstrument.

1069 Kapitel I. F. I. 1.
1070 Kapitel II. A. I. 3. b) und Kapitel II. C. I. 2. b).
1071 BayLT-Drs.17/20425, 82 („Gesichtsfelderkennung").
1072 Zu anderen biometrischen Erkennungssystemen siehe Kapitel I. C. I. 1.
1073 Nach Art. 3 Nr. 39 KI-VO ist ein Emotionserkennungssystem ein „KI-System, das dem Zweck dient, Emotionen oder Absichten natürlicher Personen auf der Grundlage ihrer biometrischen Daten festzustellen oder daraus abzuleiten"; vgl. auch Kapitel I. C. I. 2.

4. Ausdrückliche Nennung der Art biometrischer Merkmale (Gesichtsmerkmale)

Die Rechtsgrundlage muss auch zum Ausdruck bringen, dass nicht nur personenbezogene, sondern gerade biometrische Daten verarbeitet werden. Dies ergibt sich aus dem Verfassungsrecht,[1074] jedenfalls aber aus der JI-Richtlinie[1075]. Den Gesichtsmerkmalen kommt gegenüber anderen biometrischen Merkmalen darüber hinaus eine Sonderstellung zu.[1076] Im Vergleich zu verhaltensbezogenen (dynamischen) Merkmalen wie etwa Stimme, Unterschrift oder Anschlagrhythmus der Tastatur handelt es sich bei Gesichtsmerkmalen um physische biometrische Merkmale: Das Gesicht ist angeboren und weitgehend unveränderlich. Daher können durch Gesichtserkennung gewonnene Informationen eine besondere Persönlichkeitsrelevanz aufweisen. Dem Gesicht kommt auch eine herausgehobene Stellung gegenüber anderen physischen biometrischen Merkmalen wie etwa Fingerabdrücken zu, denn das Gesicht ist selbst aus einer Distanz leicht erkennbar, auf Fotos oder Videos einfach heimlich erfassbar und kann schwerlich versteckt werden, ohne Aufsehen zu erregen. Daher sollte die Rechtsgrundlage nicht nur zu erkennen geben, dass biometrische Merkmale verwendet werden,[1077] sondern die Verarbeitung von Gesichtsmerkmalen benennen. Wenn – wie nach hier vertretener Auffassung – allerdings bereits das technische Eingriffsinstrument (automatisierte Gesichtserkennung) genau benannt werden muss, ist dadurch zugleich auch die Verarbeitung biometrischer Gesichtsmerkmale offengelegt.

II. Verfahrensregelungen

1. Benachrichtigungs-, Kennzeichnungs- und Löschpflichten

Festzulegen ist zudem eine Benachrichtigungspflicht mit Blick auf die Person, gegen die nach einer Gesichtserkennungssuche weiterermittelt wird.[1078] Dabei ist es kriminalpolitisch empfehlenswert, die Vorschrift des

1074 Kapitel II. A. I. 3. b) und Kapitel II. C. I. 2. d).
1075 Kapitel II. B. I. 2. a).
1076 Hierzu Kapitel II. A. I. 2. b) dd).
1077 Wie etwa Art. 61 Abs. 2 BayPAG.
1078 Hierzu Kapitel II. A. I. 3. c) bb). Wie bereits angesprochen, ist eine Benachrichtigung der anderen Personen (Nichttreffer sowie Treffer, die dann aber nicht als

§ 101 StPO, die einheitlich Verfahrensregeln für verdeckte Maßnahmen festlegt, zu erweitern und die neu zu schaffende Rechtsgrundlage dort aufzuführen (zur Benachrichtigungspflicht siehe § 101 Abs. 4 bis 7 StPO).

Auch die Pflicht zur Kennzeichnung personenbezogener Daten (§ 101 Abs. 3 StPO) und Vorgaben für die Löschung der erlangten Daten (§ 101 Abs. 8 StPO) sollten übernommen werden, um die durch den Einsatz von Gesichtserkennung erlangten sensiblen Informationen zu schützen.

2. Richtervorbehalt

Eine Bewilligung durch ein Gericht könnte, wenn nicht bereits aus verfassungsrechtlichen,[1079] so doch zumindest aus kriminalpolitischen Erwägungen vorgeschrieben werden. Zwar ist das Rechtsinstitut des Richtervorbehalts, jedenfalls in seiner gegenwärtigen Ausgestaltung,[1080] zu Recht erheblicher Kritik ausgesetzt. Problematisiert wird insbesondere, dass aufgrund mangelnder Zeit, mangelnder Spezialisierung der Ermittlungsrichter und mangelnder Anreize nur ein geringer Teil der Anträge abgelehnt wird,[1081] und dies, obwohl die Qualität vieler Anträge empirischen Untersuchungen zufolge fragwürdig ist[1082]. Der Richtervorbehalt sei zu einem „Placebo"[1083] verkommen, zu einem „schlichten Feigenblatt ohne nennenswerte eingriffs-

---

Verdächtige identifiziert wurden) verfassungsrechtlich nicht angezeigt. Sie wäre nicht durchführbar und im Übrigen müssten für eine Benachrichtigung Namen und Adressen dieser Personen anhand der INPOL-Eintragung festgestellt werden; das würde den Grundrechtseingriff noch vertiefen. Siehe erneut zur Vereinbarkeit einer solchen Ausnahme von der Benachrichtigungspflicht für nur unerheblich betroffene Personen mit Art. 13 JI-RL *Schindler*, Biometrische Videoüberwachung, 2021, 717.

1079 Kapitel II. A. I. 3. c) aa)

1080 Dies betont *Voßkuhle*, in: Merten/Papier, Handbuch der Grundrechte, Bd. V, 2013, § 131 Rn. 100.

1081 Überblick über die Schwächen der derzeitigen Ausgestaltung des Richtervorbehalts etwa bei *Voßkuhle*, in: Merten/Papier, Handbuch der Grundrechte, Bd. V, 2013, § 131 Rn. 98.

1082 Vgl. die Nachweise bei *Voßkuhle*, in: Merten/Papier, Handbuch der Grundrechte, Bd. V, 2013, § 131 Rn. 96; vgl. zu rechtstatsächlichen Untersuchungen auch *Brüning*, Der Richtervorbehalt im strafrechtlichen Ermittlungsverfahren, 2005, 195 ff.

1083 *Stadler*, ZRP 2013, 179, 180.

begrenzende Wirkung“[1084]; der Ermittlungsrichter drohe zu einer Art „Urkundsbeamten der Staatsanwaltschaft“ zu denaturieren[1085].

Aber auch wenn eine Reform des Richtervorbehalts[1086] wünschenswert wäre – selbst in seiner gegenwärtigen schwachen Ausgestaltung kann das Rechtsinstitut zumindest einen gewissen Schutz für die von Gesichtserkennung Betroffenen bieten. Dies gilt insbesondere mit Blick auf rechtliche Vorgaben, die nicht der Wertung zugänglich sind und bei denen daher weniger die Gefahr eines „Abnickens“ des Antrags auf Einsatz von Gesichtserkennung besteht. Eine Ermittlungsrichterin könnte etwa sicherstellen, dass die Strafverfolgungsbehörden nur zertifizierte technische Systeme einsetzen oder dass nur qualifizierte Personen den Abgleich und die Identifizierung vornehmen[1087]. Eine Richterin könnte zudem prüfen, ob überhaupt der Verdacht einer Straftat (und nicht etwa nur einer Ordnungswidrigkeit) mit Blick auf die auf dem Suchbild zu sehende Person vorliegt.

3. Subsidiaritätsklausel

Ob ausdrücklich die Subsidiarität[1088] der Identifizierung durch automatisierte Gesichtserkennung geregelt werden sollte, ist hingegen zweifelhaft.[1089] Zwar enthält die Mehrzahl der Vorschriften, die heimliche Ermitt-

1084 *Lilie*, ZStW 111 (1999), 807, 814; vgl. auch *Jahn,* NStZ 2007, 255, 259; *Kutscha*, NVwZ 2003, 1296, 1300.

1085 *Schünemann*, ZStW 114 (2002), 1, 20; vgl. auch *Heghmanns*, GA 2003, 433, 440.

1086 Zusammenfassend zu möglichen Reformen *Voßkuhle*, in: Merten/Papier, Handbuch der Grundrechte, Bd. V, 2013, § 131 Rn. 100; siehe auch bereits *Brüning*, ZIS 2006, 29, 34 f.; *Gusy*, ZRP 2003, 275, 276 ff.; *Helmken*, StV 2003, 193, 196; *Lilie*, ZStW 111 (1999), 807, 816; *Amelung*, Rechtsschutz gegen strafprozessuale Grundrechtseingriffe, 1976, 65.

1087 Zu dieser Vorgabe sogleich unter III. 1.

1088 Zu Subsidiaritätsklauseln auch Kapitel II. C. I. 1. a).

1089 Eine Subsidiaritätsklausel kann neben dem aus Art. 10 JI-RL, § 48 Abs. 1 BDSG folgenden Erfordernis der „unbedingten Erforderlichkeit“ der Datenverarbeitung eine eigenständige Bedeutung haben. Wenn die „unbedingte Erforderlichkeit“ beispielsweise als eine besonders strenge Verhältnismäßigkeitsprüfung verstanden wird (zum Streit Kapitel II. B. I. 2. b)), dann wäre sie zu bejahen, wenn kein *gleich geeignetes* Mittel zur Identifizierung zur Verfügung steht und die Gesichtserkennungsmaßnahme wäre daher – wenn die übrigen Voraussetzungen vorliegen – zulässig. Dagegen könnte in diesem Fall aufgrund einer Subsidiaritätsklausel der Einsatz automatisierter Gesichtserkennung dennoch unzulässig sein, denn eine Subsidiaritätsklausel stellt nicht darauf ab, ob es gleich geeignete Maßnahmen gibt, sondern ob andere Maßnahmen in einem bestimmten Maße *weniger geeignet* sind

lungsmethoden regeln,[1090] eine Subsidiaritätsklausel; damit soll sichergestellt werden, dass diese Maßnahmen nur nachrangig zur Anwendung kommen. Bei der automatisierten Gesichtserkennung ist eine solche abstrakte Nachrangigkeit aber nicht immer sinnvoll. Denn obwohl die automatisierte Gesichtserkennung eine eingriffsintensive und fehleranfällige Maßnahme ist (daher wird in dieser Arbeit eine strenge Regulierung vorgeschlagen), sind gerade ihre *Alternativen*, vor allem die Identifizierung (allein) durch Augenzeugen, unter Umständen sogar noch fehleranfälliger. Selbst wenn ein Zeuge bereits angibt, einen Verdächtigen erkannt zu haben, kann es sinnvoll sein, dennoch eine Gesichtserkennungsrecherche durchzuführen. Das kann etwa der Fall sein, wenn zwischen dem Geschehen und der Identifizierung durch den Zeugen ein großer Zeitabstand liegt. Eine Subsidiaritätsklausel würde aber generell die Nachrangigkeit der automatisierten Gesichtserkennung anordnen, sodass unklar wäre, ob sie in solch einem Fall noch durchgeführt werden dürfte.

4. Verfahren der Identifizierung

Um Ermittlungen gegen Unschuldige so weit wie möglich zu verhindern, sollten besondere Schutzmaßnahmen festgelegt werden. Vor dem Hintergrund der begrenzten menschlichen Fähigkeit zur Gesichtserkennung[1091] sollte die Rechtsgrundlage regeln, dass nur ausgebildete Lichtbildsachverständige und -experten das Gesichtserkennungssystem verwenden und anhand der Kandidatenliste den Verdächtigen identifizieren oder den Verdacht einer Personenidentität feststellen dürfen.[1092] Dies wird, soweit er-

(z. B. „erheblich weniger erfolgversprechend oder wesentlich erschwert" bei § 98a Abs. 1 StPO oder „wesentlich erschwert oder aussichtslos" bei § 100a Abs. 1 StPO).

1090 Eine Ausnahme bilden etwa § 98c StPO und § 163g StPO (automatische Kennzeichenerfassung).

1091 Kapitel III. B. II. 2. a).

1092 Eine besondere Qualifikation der Personen, die eine strafprozessuale Maßnahme vornehmen, regelt beispielsweise auch § 110d S. 2 StPO, wonach bei Beantragung der Maßnahme darzulegen ist, dass die handelnden Polizeibeamten auf den Einsatz umfassend vorbereitet wurden; zur Begründung dieses Erfordernisses BT-Drs. 19/16543, 12. Vgl. auch § 22 Abs. 6 S. 2, § 23 Abs. 4 S. 2 und § 24 Abs. 5 S. 2 TTDSG, die auf Seiten der Anbieter von Telemediendiensten regeln, dass jedes Auskunftsverlangen der Behörden durch eine „Fachkraft" zu prüfen ist (allerdings ohne den Begriff zu definieren).

sichtlich, bei der Verwendung des BKA-GES bereits praktiziert,[1093] ist allerdings nicht gesetzlich geregelt, sodass diese Praxis jederzeit aufgeweicht werden könnte. Auch könnte gegenwärtig eine Polizeibehörde, die selbst ein Gesichtserkennungssystem zur Durchsuchung des lokalen Lichtbildbestands anschafft, einen ungeschulten Polizisten mit dem Abgleich und der Identifizierung betrauen. Dies ist zu verhindern. Auch könnte ausdrücklich geregelt werden, dass die Identifizierung nicht durch eine Person erfolgen darf, die in die Ermittlungstätigkeit dieses Fall involviert ist und daher womöglich voreingenommen ist und vorschnell einen Verdacht annehmen könnte, um einen Ermittlungsansatz zu generieren.[1094] Die Rechtsgrundlage sollte zudem vorsehen, dass im Antrag für den Gerichtserkennungseinsatz darzulegen ist, dass die Personen, die den Abgleich und die Identifizierung vornehmen sollen, hierfür qualifiziert sind. Hier könnte entweder direkt an die Qualifikation als Lichtbildsachverständiger oder -experte[1095] angeknüpft werden („Eine solche Maßnahme dürfen nur Lichtbildsachverständige und Lichtbildexperten treffen") oder – wie in § 110d S. 2 StPO[1096] – eine allgemeinere Formulierung gewählt werden („Eine solche Maßnahme dürfen nur hierfür besonders qualifizierte Personen treffen"). Die handelnden Personen müssen namentlich oder nach ihrer Funktion im Antrag individualisierbar bezeichnet werden.[1097]

Zudem sollte ein echter 4-Augen-Vergleich festgelegt werden. Derzeit wird, soweit ersichtlich, der 4-Augen-Vergleich im Rahmen der Gesichtserkennung so praktiziert, dass ein Experte aus der Kandidatenliste den Verdächtigen auswählt und der zweite Experte lediglich dieses Ergebnis bestätigt oder verwirft. Durch die erste Identifizierung wird aber bereits ein „Anker" geworfen. Stattdessen sollte festgelegt werden, dass die Experten unabhängig voneinander[1098] – also ohne das Ergebnis des anderen zu kennen – dieselbe Person identifizieren bzw. einen Verdacht der Personenidentität feststellen müssen, bevor gegen sie ermittelt werden darf.

Die KI-Verordnung regelt hier keine ausreichenden Schutzmechanismen. Art. 14 Abs. 5 KI-VO schreibt zwar vor, dass zwei natürliche Personen den Treffer bestätigen müssen, allerdings ist diese Vorgabe nicht als Pflicht

1093 Kapitel II. F. I. 2. c)
1094 Kapitel III. B. III.
1095 Zur Ausbildung für diese Qualifikation siehe bereits Kapitel I. F. I. 2. c).
1096 In § 110d StPO S. 2 StPO ist geregelt, dass in dem Antrag darzulegen ist, dass die handelnden Polizeibeamten auf den Einsatz „umfassend vorbereitet wurden".
1097 So mit Blick auf § 110d S. 2 StPO *Rückert/Goger*, MMR 2020, 373, 377.
1098 Vgl. auch die Regelung in § 5 Abs. 1 S. 1 TPG.

der Betreiber ausgestaltet, sondern als (technische) Designvorgabe adressiert an den Anbieter des KI-Systems.[1099] Davon abgesehen ist die Vorgabe, dass diese natürlichen Personen die „notwendige Kompetenz, Ausbildung und Befugnis" haben müssen, wenig konkret und daher jedenfalls für den sensiblen Bereich der Strafverfolgung nicht ausreichend. Auch Art. 26 Abs. 10 Uabs. 3 S. 2 KI-VO bietet keinen genügenden Schutz.[1100]

Wie bereits erwähnt, sollte das Erfordernis der Überprüfung von Treffern einer Kandidatenliste durch Menschen allerdings kritisch hinterfragt werden, wenn in Zukunft deutlich wird, dass die Technologie leistungsfähiger ist als (auch geschulte) Menschen; hierzu sogleich unter IV.

III. Besonderer Schutz der Versammlungsfreiheit

Zusätzliche Voraussetzungen sollte die Rechtsgrundlage für automatisierte Gesichtserkennung festgelegen, wenn es um die Identifizierung von Personen geht, die verdächtigt werden, im Zusammenhang mit einer Versammlung eine Straftat begangen zu haben. Wegen ihres objektiv-rechtlichen Gehalts entfaltet die Versammlungsfreiheit Ausstrahlungswirkungen auf die gesamte Rechtsordnung.[1101] Auch der EGMR hat in seiner Entscheidung zum Einsatz automatisierter Gesichtserkennung Glukhin v. Russland den Versammlungskontext besonders hervorgehoben.[1102] Die Befürchtung, dass beim Verdacht jeder beliebigen, noch so geringfügigen Straftat Videomaterial von einer Versammlung nachträglich per Gesichtserkennung ausgewertet wird, kann Bürgerinnen und Bürger von der Teilnahme abhalten. Der Verdacht einer Straftat kann mitunter schnell begründet sein: Wird bei leichtem Anrempeln eines Polizisten wegen tätlichen Angriffs auf Vollstreckungsbeamte nach § 114 StGB ermittelt, bei einer überspitzten Meinungsäußerung wegen eines Äußerungsdelikts? Der Einsatz automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger wegen Straftaten im Zusammenhang mit einer Versammlung sollte daher beschränkt werden auf Ermittlungen wegen Straftaten eines bestimmten Gewichts.[1103]

1099 Hierzu Kapitel II. B. I. 1. b) gg).
1100 Kapitel II. B. I. 1. d) cc).
1101 Kapitel II. A. II. 1. b).
1102 Kapitel II. B. II. 1. und 2.
1103 In diese Richtung auch Report of the United Nations High Commissioner for Human Rights, Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests, UN

Angemessen erscheint eine Beschränkung auf Straftaten von „auch im Einzelfall erheblicher Bedeutung" (vgl. §§ 100g Abs. 1 S. 1 Nr. 1, 100i Abs. 1, 100k Abs. 1 S. 1 StPO). Eine Straftat von erheblicher Bedeutung muss nach einhelliger Auffassung mindestens dem Bereich der mittleren Kriminalität zuzurechnen sein, den Rechtsfrieden empfindlich stören und dazu geeignet sein, das Gefühl der Rechtssicherheit der Bevölkerung erheblich zu beeinträchtigen.[1104]

IV. Umsetzung in einer Rechtsgrundlage

1. Regelungstechnik

a) Orientierung an der Regelungstechnik der KI-Verordnung nicht empfehlenswert

Eine Orientierung an der Regelungstechnik der KI-Verordnung mit Blick auf biometrische Fernidentifizierungssysteme ist nicht ratsam. Die Verordnung enthält eine einheitliche Definition und Regelung für alle biometrischen Fernidentifizierungssysteme (z. B. Gesichtserkennung, Gangerkennung). Welche Methoden der biometrischen Erkennung solche der „Fernidentifizierung" sind, ist aber nicht klar abzugrenzen;[1105] eine solche allgemeine Definition würde daher ohne Not Rechtsunsicherheit hervorrufen. Zudem werfen unterschiedliche Methoden unterschiedliche Probleme auf. Allein bei der Gesichtserkennung ergeben sich, wie diese Arbeit zeigt, eine Reihe spezifischer Risiken, die es als solche zu erkennen und zu regeln gilt.[1106] Eine allgemeine Rechtsgrundlage für biometrische Fernidentifizierung erscheint vor diesem Hintergrund nicht ratsam; automatisierte Gesichtserkennung sollte als eigene Maßnahme geregelt werden. Sofern in der Strafverfolgung ein Erfordernis der biometrischen Fernidentifizierung mit anderen Methoden (z. B. Stimmerkennung, Gangerkennung) besteht, sollten die jeweiligen Risiken zunächst ausführlich und differenziert untersucht und erst dann eine darauf zugeschnittene Rechtsgrundlage geschaffen werden.

Doc. A/HRC/44/24, 2020, 10 („Existing recordings should only be used for the identification of assembly participants who are suspects of serious crimes.").

1104 BVerfGE 103, 21 (34) mwN. Näher zum Begriff der Straftat von auch im Einzelfall erheblicher Bedeutung MüKoStPO/*Rückert*, 2. Aufl. 2023, StPO § 100g Rn. 57 ff.

1105 Kapitel I. C. I. 1.

1106 Siehe nur Kapitel III. B. II. 2. f) zu Folgeproblemen bei Wahllichtbildvorlagen.

Auch die pauschale Unterscheidung zwischen Echtzeit- und nachträglicher Erkennung in der KI-Verordnung sollte nicht als Regelungstechnik übernommen werden.[1107] Diese grobe Einordnung wird den Besonderheiten der einzelnen Einsatzvarianten nicht gerecht: Die Verwendung nachträglicher Gesichtserkennung zur Nachverfolgung des Weges eines Verdächtigen auf öffentlichen Videoaufzeichnungen birgt andere Gefahren als der Einsatz nachträglicher Gesichtserkennung zur Identifizierung unbekannter Verdächtiger anhand von Lichtbilddatenbanken. Jedes Einsatzszenario von Gesichtserkennung muss eigenständig betrachtet, vertieft untersucht und geregelt werden. Für den Einsatz automatisierter Gesichtserkennung gerade zum Zweck der Identifizierung unbekannter Verdächtiger sollte daher eine eigenständige Rechtsgrundlage geschaffen werden. Für die Verwendung automatisierter Gesichtserkennung in anderen Szenarien bedarf es zunächst weiterer vertiefter (u. a. rechtswissenschaftlicher) Untersuchungen.

b) Keine Ergänzung von § 98c StPO, sondern eigene Regelung

Der Einsatz automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger sollte nicht in § 98c StPO, sondern in einer eigenständigen Rechtsgrundlage geregelt werden. Die Maßnahme macht eine Vielzahl zusätzlicher Vorkehrungen nötig, die für einen „einfachen Datenabgleich", wie ihn § 98c StPO vorsieht, nicht erforderlich sind (z. B. Verwendung nur durch ausgebildete Lichtbildsachverständige und -experten, besondere technische Anforderungen an die verwendeten Systeme).

Die Vorgaben des Art. 10 JI-RL, § 48 BDSG (Erfordernis der „unbedingten Erforderlichkeit" der Datenverarbeitung sowie geeignete Schutzgarantien)[1108] sollten, soweit wie möglich, direkt in der Rechtsgrundlage, ansonsten anderweitig gesetzlich verankert werden. Nur wo dies nicht möglich oder sinnvoll erscheint (z. B. Erfordernis von Schulungen), sollte auf innerbehördliche Regelungen ausgewichen werden. Auch die Vorgabe des Art. 26 Abs. 10 Uabs. 3 S. 2 KI-VO („Es muss sichergestellt werden, dass die Strafverfolgungsbehörden keine ausschließlich auf der Grundlage der Ausgabe solcher Systeme zur nachträglichen biometrischen Fernidentifizierung beruhende Entscheidung, aus der sich eine nachteilige Rechtsfolge

1107 Siehe bereits *Hahn*, ZfDR 2023, 142, 155 ff., 161.
1108 Kapitel II. B. I. 2. b).

für eine Person ergibt, treffen.")[1109] sollte – auch wenn sie unmittelbar gilt (Art. 288 Abs. 2 AEUV) – direkt in der Rechtsgrundlage zum Einsatz automatisierter Gesichtserkennung verankert werden. Um die in einer Hinsicht darüberhinausgehenden Vorgaben des Art. 11 JI-RL zu wahren,[1110] sollte diese Formulierung um den Passus *„oder eine erhebliche Beeinträchtigung"* ergänzt werden.

2. Vorschlag für eine Formulierung

Die neue Rechtsgrundlage für den Einsatz automatisierter Gesichtserkennung zur Identifizierung unbekannter Verdächtiger könnte als § 163h StPO in die Strafprozessordnung eingefügt werden und folgendermaßen lauten:

> **§ 163h StPO Identifizierung unbekannter Verdächtiger mit automatisierter Gesichtserkennung**
> (1) Zur Ermittlung der Identität unbekannter Verdächtiger dürfen Gesichtserkennungssysteme verwendet werden, die anhand biometrischer Merkmale Lichtbilder verarbeiten (automatisierte Gesichtserkennung), wenn dies unbedingt erforderlich ist. Ein Abgleich eines Lichtbilds des Verdächtigen darf nur mit Lichtbildern der [nähere Bezeichnung der Datenbanken] vorgenommen werden.
> (2) Weitere Ermittlungen gegen eine mit automatisierter Gesichtserkennung identifizierte Person sind nur zulässig, wenn zwei natürliche Personen unabhängig voneinander die Personenidentität oder den Verdacht der Personenidentität mit dem Verdächtigen festgestellt haben. Eine Entscheidung, aus der sich eine nachteilige Rechtsfolge für eine Person ergibt, darf nicht ausschließlich auf der Grundlage der Ausgabe eines Gesichtserkennungssystems getroffen werden.
> (3) Eine Maßnahme nach Absatz 1 und eine Feststellung nach Absatz 2 Satz 1 dürfen nur hierfür besonders qualifizierte Personen treffen.
> (4) Eine Maßnahme nach Absatz 1 darf nur durch das Gericht, bei Gefahr im Verzug auch durch die Staatsanwaltschaft angeordnet werden. In dem Antrag ist darzulegen, dass die mit der Maßnahme nach Absatz 1 und der Feststellung nach Absatz 2 Satz 1 betrauten Personen die erforderliche Qualifikation besitzen.

1109 Kapitel II. B. I. 1. d) cc).
1110 Kapitel II. B. I. 2. c).

(5) Dient die automatisierte Gesichtserkennung der Identifizierung eines Verdächtigen wegen einer im Zusammenhang mit einer Versammlung begangenen Tat, so ist dies nur bei einer Straftat von auch im Einzelfall erheblicher Bedeutung zulässig.
(6) Für eine Maßnahme nach Absatz 1 dürfen nur Gesichtserkennungssysteme verwendet werden, die nach dem jeweiligen Stand der Technik ein Höchstmaß an Genauigkeit aufweisen und entsprechend zertifiziert sind. Die Bundesregierung wird ermächtigt, durch Rechtsverordnung Regelungen zu treffen über
1. die für eine Zertifizierung zuständige, von den Strafverfolgungsbehörden unabhängige Stelle,
2. die technischen und organisatorischen Anforderungen an das Zertifizierungsverfahren und
3. die Dauer der Gültigkeit eines Zertifikats.

In § 101 Abs. 1 StPO sollte „§ 163h" ergänzt werden, sodass die Kennzeichnungs- und Löschpflichten auch für diese Vorschrift gelten.

In § 101 Abs. 4 („Von den in Absatz 1 genannten Maßnahmen sind im Falle […] zu benachrichtigen") sollte ergänzt werden: „Nr. 14 des § 163h die betroffene Person, gegen die nach Abgleich der Lichtbilder weitere Ermittlungen geführt wurden".

C. Weitere Empfehlungen

I. Schulungen und Überarbeitung der RiStBV

Um Fehler im Zusammenhang mit dem Einsatz automatisierter Gesichtserkennung so weit wie möglich zu verhindern, müssen Ermittler im Umgang mit den Ergebnissen von Gesichtserkennungsrecherchen geschult sein. Die Fehleranfälligkeit der Technologie[1111] und vor allem die Quellen menschlicher Fehler[1112] müssen ihnen bewusst sein. Zu diesem Zweck sollten etwa Fälle des Einsatzes automatisierter Gesichtserkennung, in denen (wie sich später herausstellte) gegen Unbeteiligte ermittelt wurde, herangezogen und daraufhin untersucht werden, ob und wie dies hätte verhindert werden können.

1111 Kapitel III. B. II. 1. und Kapitel I. E. IV.
1112 Kapitel III. B. II. 2. und 3.

Zudem wäre es ratsam, die RiStBV um spezifische Vorschriften zum Einsatz von Gesichtserkennung zu ergänzen. So könnte etwa in Nr. 18 RiStBV (Gegenüberstellung und Wahllichtbildvorlage) festgelegt werden, dass bei einer Gegenüberstellung oder Wahllichtbildvorlage dem Zeugen nicht offenbart werden darf, dass ursprünglich Gesichtserkennung zur Identifizierung des Verdächtigen verwendet wurde. Auch könnte in den RiStBV geregelt werden, dass zum Gesichtserkennungsabgleich nur Bilder des Verdächtigen (keine Doppelgänger; keine handgezeichneten oder computergenerierten zusammengesetzten Gesichtern auf der Grundlage von Zeugenbeschreibungen) verwendet werden dürfen.

II. Kontrolle und Evaluation

Der Einsatz automatisierter Gesichtserkennung kann unbeabsichtigte Folgen mit sich bringen, insbesondere für die Selektivität der Strafverfolgung und für Unbeteiligte, die Ermittlungsmaßnahmen unterworfen werden.[1113] Auch kann sich der Einsatz automatisierter Gesichtserkennung auf die Wahrnehmung der Strafverfolgungsbehörden in der Öffentlichkeit auswirken. Gesichtserkennung ist eine heimliche Maßnahme, die zumindest in den Medien mit Fehlern und Rassismus assoziiert wird;[1114] bei fehlender Transparenz und Akzeptanz der Maßnahmen könnte das Vertrauen in die Polizei womöglich sinken.

Um dem entgegenzuwirken, sollte eine Evaluationskommission eingesetzt werden, die den Einsatz automatisierter Gesichtserkennung kontrolliert und evaluiert.[1115] Die Kommission sollte pluralistisch und divers besetzt und insbesondere die Disziplinen Rechtswissenschaft, Kriminologie, Informatik, Soziologie und Psychologie sollten vertreten sein. Damit soll keine Kontrolle jeder Einzelmaßnahme, sondern vielmehr des „Systems" Gesichtserkennung als Ganzem ermöglicht werden. Beispielsweise könnte die Evaluationskommission untersuchen bzw. untersuchen lassen, ob und in welchen Fällen es im Zusammenhang mit Gesichtserkennung zu Ermittlungen gegen Unbeteiligte kommt und ob dies bei bestimmten Personengruppen häufiger vorkommt. (Diese Erkenntnisse können wiederum zur Schulung von Polizisten verwendet werden, um für Probleme zu sensibili-

1113 Kapitel III. A. und B.
1114 Kapitel III. C. III. 3. c) und Kapitel III. C. IV. 2.
1115 Kapitel II. A. I. 3. c) cc.) und Kapitel III. C. IV. 2.

sieren.) Auf Basis dieser Erkenntnisse könnte die Kommission Vorschläge dafür erarbeiten, wie Fehler in der Mensch-Maschine-Interaktion verhindert werden können. Wichtig erscheint zudem, empirisch erforschen zu lassen, welche Delikte und welche Menschen mit Gesichtserkennung verstärkt verfolgt werden. Auch könnte die Kommission verfolgen und analysieren lassen, wie der Einsatz von Gesichtserkennung durch die Polizei in der Bevölkerung wahrgenommen wird.

Eine solche Kontrolle und Evaluation auf einer Meta-Ebene würde dazu beitragen, unbeabsichtigte Auswirkungen des Einsatzes von Gesichtserkennung frühzeitig zu erkennen. Außerdem könnte eine solche unabhängige Überprüfung das Vertrauen der Bevölkerung in den polizeilichen Einsatz neuer Strafverfolgungstechnologien stärken.

III. Bericht für die Öffentlichkeit

Für die Öffentlichkeit sollte die Kommission zudem einen jährlichen Bericht über den Einsatz von Gesichtserkennung in der Strafverfolgung erarbeiten. Darin könnten die Befunde eigener Untersuchungen enthalten sein, aber auch Informationen der Zertifizierungsstelle zur Anzahl der eingesetzten Systeme und vor allem zu Fehleranfälligkeit und Verzerrungen. Mit einem solchen Bericht bestünde eine deutlich solidere Basis für eine demokratische Debatte über die Verwendung von Gesichtserkennung und ihre unbeabsichtigten Folgen, als dies derzeit der Fall ist. Gesichtserkennung würde, so die Hoffnung, weniger als dystopische Überwachungstechnologie wahrgenommen, die die Behörden „heimlich" einführen und verwenden, sondern als eine Maßnahme, die auf rechtlicher Grundlage eingesetzt und umfassend kontrolliert und evaluiert wird.

IV. Beobachtung technologischer und gesellschaftlicher Entwicklungen

Von Seiten des Gesetzgebers sollten der technologische Fortschritt und gesellschaftliche Veränderungen gerade mit Blick auf den Einsatz automatisierter Gesichtserkennung beobachtet werden.

So sollte etwa verfolgt werden, wie sich die Leistungsfähigkeit von Gesichtserkennungssystemen – insbesondere im Vergleich zu der von Menschen – entwickelt. Wie bereits erwähnt, sollte das Erfordernis der Überprüfung von Treffern einer Kandidatenliste durch Menschen allerdings

kritisch hinterfragt werden, wenn in Zukunft deutlich wird, dass die Technologie leistungsfähiger ist als (auch geschulte) Menschen. Denn dann würde das Auswählen des Verdächtigen aus der Kandidatenliste durch Lichtbildsachverständige oder -experten zu *mehr Fehlern* und *mehr Ermittlungen gegen Unschuldige* führen, als wenn nur der Top-1-Treffer des Gesichtserkennungssystems direkt an den Ermittler weitergeleitet würde. Mit Art. 14 Abs. 5 S. 1 KI-VO (wenn man ihn überhaupt als materielle Vorgabe begreift) wäre dies allerdings nur dann vereinbar, wenn die Ermittler eine „Ausbildung" („training") in der Anwendung des Systems haben.

Ob bzw. wann die Technologie tatsächlich leistungsfähiger ist als geschulte Menschen, muss jedoch noch weiter erforscht werden. Auch müsste eine solche Umstellung der Abläufe (Top-1-Treffer wird direkt an Ermittler weitergeleitet) erst recht äußerst kritisch untersucht, begleitet und evaluiert werden. Insbesondere wird sich die Frage stellen, wie ein Automation bias so weit wie möglich verhindert werden kann. Diese Frage stellt sich bei der Weiterleitung von nur einem Treffer mit noch höherer Dringlichkeit, als wenn – wie gegenwärtig der Fall – die Lichtbildexperten und -sachverständigen aus einer Liste den Kandidaten selbst eine Person aktiv auswählen müssen. Auch stellen sich Folgefragen für das Gerichtsverfahren: Gerade wenn ein Gesichtserkennungssystem tatsächlich besser als der Mensch ist, kann es zu Fällen kommen, in denen das Ergebnis eben nicht mehr von einem Menschen überprüft und nachvollzogen werden kann. Wenn das System – verlässlicher als der Mensch – dann eine Person als Verdächtigen identifiziert und sich bei den Ermittlungen keine anderen Beweise ergeben, kommt es für die Verurteilung entscheidend darauf an, ob es sich um den Verdächtigen handelt oder nicht. Kann das Ergebnis des Gesichtserkennungssystems dann tatsächlich auch als *Beweis* herangezogen werden statt nur als ermittlungsunterstützender Hinweis? Die Frage, wie in Gerichtsverfahren mit nicht erklärbaren Ergebnissen von KI-Systemen umzugehen ist, bedarf noch intensiver weiterer Forschung.

D. Schlusswort

„The real problem is not whether machines think
but whether men do."
– B. F. Skinner[1116]

Diese Arbeit versteht sich als Kritik eines unreflektierten Einsatzes wirkmächtiger neuer Technologien. Verfassungsrechtliche Grundsätze und das Bewusstsein für Risiken können dabei allzu schnell in den Hintergrund treten. Dabei besteht nicht nur die Gefahr, dass Menschen die Technologien ohne Berücksichtigung möglicher Folgen entwickeln und gedankenlos anwenden. Ebenso bedenklich ist es, wenn der Gesetzgeber die Einführung unbeachtet geschehen lässt. Die Entscheidung über die Verwendung folgenreicher neuer Technologien in der Strafverfolgung muss vom demokratisch legitimierten Gesetzgeber durchdacht und bewusst getroffen sein.

Mit Blick auf automatisierte Gesichtserkennung war dies jedoch nicht der Fall. Bereits seit 2008 setzt das BKA ein Gesichtserkennungssystem zur Identifizierung unbekannter Verdächtiger ein, Bundespolizei und Landespolizeibehörden haben nachgezogen. Einige Polizeibehörden schaffen sich mittlerweile eigene Systeme an. Jedes Jahr werden zehntausende Suchanfragen durchgeführt – Tendenz steigend. Diese Entwicklung hat sich vollzogen ohne demokratischen Diskurs, ohne Schaffung einer Rechtsgrundlage und ohne die Beteiligung von Rechtswissenschaft und Kriminologie.

Diese Arbeit hat das Anliegen, eine Debatte über die Regulierung automatisierter Gesichtserkennung in der Strafverfolgung anzustoßen. Damit ist auch die Hoffnung verbunden, dass mit Blick auf neue Technologien der Fokus weniger auf dystopische, weit entfernte Zukunftsszenarien gerichtet wird. Stattdessen sollten konkrete Risiken in den Blick genommen werden, die bereits jetzt für Menschen und die Gesellschaft als Ganze bestehen. Das Recht darf hier nicht untätig zusehen.

1116 *Skinner*, Contingencies of Reinforcement, 1969, Kap. 9.