bidt Bayerisches Forschungsinstitut für Digitale Transformation
EIN INSTITUT DER BAYERISCHEN AKADEMIE DER WISSENSCHAFTEN

IMPULSE

# Gesichtserkennung

## Ein Diskussionsbeitrag zur Regulierung der Technologie

**AutorInnen:** Nikolaus Bauer, Jan Gogoll, Niina Zuber

## Impressum

**bidt Impulse Nr. 3**

**bidt – Bayerisches Forschungsinstitut**
**für Digitale Transformation**
Gabelsbergerstraße 4
80333 München
www.bidt.digital

**Koordination**
Margret Hornsteiner, Nadine Hildebrandt
dialog@bidt.digital

**Gestaltung**
made in – Design und Strategieberatung | www.madein.io

**Layout**
Joseph & Sebastian | www.josephundsebastian.com

**Veröffentlichung**
Dezember 2021

**ISSN:** 2701-2395
**DOI:** 10.35067/b0bj-im03

Das Bayerische Forschungsinstitut für Digitale Transformation (bidt) trägt als Institut der Bayerischen Akademie der Wissenschaften dazu bei, die Entwicklungen und Herausforderungen der digitalen Transformation besser zu verstehen. Damit liefert es die Grundlagen, um die digitale Zukunft der Gesellschaft verantwortungsvoll und gemeinwohlorientiert zu gestalten.

Mit dem Ad-hoc-Projekt „Gesichtserkennung“ möchte das bidt einen wissenschaftlichen Beitrag zur aktuellen Diskussion um die Regulierung der Technologie leisten. Das Projekt verbindet interdisziplinäre Perspektiven aus Rechtswissenschaft, Informatik und Ethik.

## Die AutorInnen

**Nikolaus Bauer** ist wissenschaftlicher Referent in der Abteilung Forschung am bidt. E-Mail: nikolaus.bauer@bidt.digital

**Dr. Jan Gogoll** ist wissenschaftlicher Referent in der Abteilung Forschung am bidt. E-Mail: jan.gogoll@bidt.digital

**Niina Zuber** ist wissenschaftliche Referentin in der Abteilung Forschung am bidt. E-Mail: niina.zuber@bidt.digital

## Abstract

Gesichtserkennung wird in der Öffentlichkeit oftmals kontrovers diskutiert. Es gibt Rufe nach einem Verbot oder einer Regulierung der Technologie. Der vorliegende Impuls möchte einen Beitrag zu dieser Diskussion leisten und aufzeigen, ob ein Verbot oder neue rechtliche Regelungen notwendig erscheinen.

*There is currently a controversial public debate about Facial Recognition, with many calling for the technology to be subject to tighter regulation and some even demanding a complete ban. This impulse paper aims to make a contribution to this debate by considering whether new regulations or a ban are justified.*

Inhalt

# 1. Einleitung

Gesichtserkennungssysteme werden zur Passkontrolle oder zum Entsperren des Mobiltelefons eingesetzt. Sie können Krankheiten und die psychische Verfassung oder das Alter erkennen, Vermisste identifizieren oder dazu eingesetzt werden, Verdächtige aufzuspüren.

Dies zeigt, dass die Technik viele Anwendungsfelder hat und Chancen bietet, aber auch Risiken birgt. Sie hilft, eine Passkontrolle effizienter zu gestalten, Krebs zu erkennen oder Verdächtige und Vermisste aufzuspüren. Gleichzeitig könnten Betroffene jedoch aufgrund ihrer psychischen Verfassung oder ihres Alters diskriminiert werden und biometrische Gesichtserkennung im öffentlichen Raum zu Einschüchterungseffekten führen (sogenannte „chilling effects").

Die Systeme der Gesichtserkennung werden technisch immer zuverlässiger. Aber bedeutet technische Zuverlässigkeit zugleich, dass die Systeme auch eingesetzt werden dürfen?

Wie soll die Gesellschaft mit den Chancen und Risiken der Technologie richtig umgehen? Bedarf es einer Regulierung der Systeme, und wenn ja, welcher? Sollten bestimmte Formen verboten werden, wie etwa der Europarat hinsichtlich sogenannter „Affekt-Erkennungstechnologie" und anderer Formen von Gesichtserkennung vorschlägt? Sollte es ein Verbot oder zumindest ein Moratorium für den Einsatz biometrischer Gesichtserkennung im öffentlichen Raum geben? Immerhin hat die EU-Kommission bereits über ein solches Moratorium nachgedacht.

Dieser Impuls versucht, Antworten auf diese Fragen zu finden und damit einen Beitrag zur aktuellen Diskussion über die Regulierung von Gesichtserkennung zu leisten.

## 2. Grundlagen der Gesichtserkennung

Allen Gesichtserkennungssystemen liegt technisch als erster Schritt das Erkennen von Gesichtern zugrunde. Dies bedeutet: Eine Software muss auf einem Foto oder in einem Video einen Bereich als Gesicht klassifizieren. Dies wird als Erkennung oder Detektion bezeichnet.

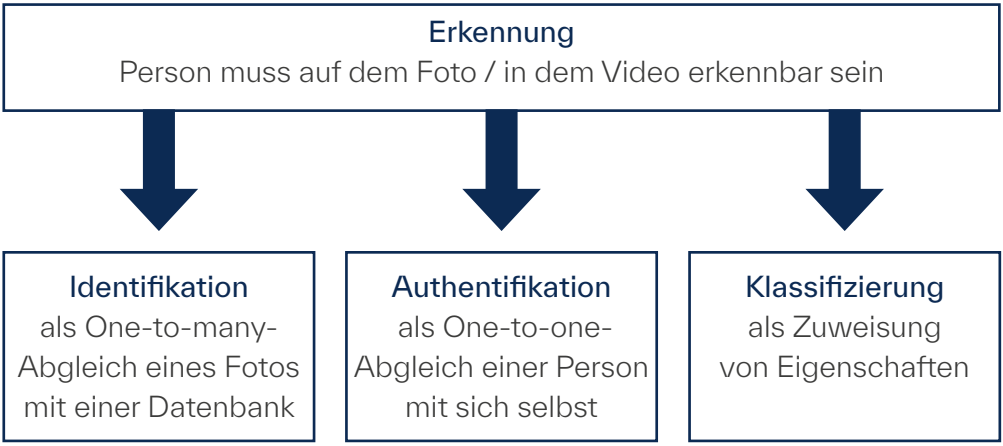
Die alleinige Detektion von Gesichtern ist meist noch kein wertvoller Anwendungsfall. Dieser entsteht durch einen Abgleich des erkannten Gesichts mit bereits hinterlegten Bildern. Gesichtserkennung vergleicht Bilder von Gesichtern, um ihre Ähnlichkeit zu bestimmen, die die Technologie mithilfe einer Bewertung von Ähnlichkeiten („similarity score“) darstellt (McLaughlin/Castro 2020).

Das Szenario einer polizeilichen Fahndung entspricht der Identifikation durch eine Gesichtserkennungstechnologie: Ein Gesicht auf einem Foto oder in einem Video soll in einer Menge von Einträgen in vorhandenen Datenbanken gefunden werden – oder es soll zumindest eine Liste von potenziell infrage kommenden Personen erstellt werden. Diese Art der Gesichtserkennung entspricht einem One-to-many-Matching.

Eine Passkontrolle oder das Entsperren eines Mobiltelefons sind Beispiele für die Authentifikation, bei der Gesichtserkennungssysteme zum Einsatz kommen können. Dazu werden biometrische Daten wie Augenabstand oder Stirnbreite mit einem hinterlegten Datensatz abgeglichen. Diese Bestätigung wird deshalb auch als One-to-one-Matching bezeichnet.

Technologien zur Gesichtserkennung lassen sich auch dazu einsetzen, eine Person bestimmten Kategorien zuzuordnen: Wie alt ist sie? Welches Geschlecht hat sie? Welchen Hautton? Welche Emotion wird aus dem Gesicht abgelesen? Um Fragen dieser Art zu beantworten, bedarf es technisch weder einer Identifikation noch einer Authentifizierung, stattdessen kategorisiert das Softwaresystem nach definierten Kriterien. Dies wird als Klassifikation („classifying“) bezeichnet. Etwa: Welches „Faltigkeitsintervall“ entspricht einem bestimmten Alter? Welcher Farbton wird welcher Hautfarbe zugeordnet? Welche Mundwinkel stellen welche emotionale Verfasstheit einer Person dar? Diese Grenzwerte können auf drei Arten zustande kommen: (1) Ein Mensch definiert manuell eine Skala. (2) Methoden des Maschinellen Lernens leiten die Grenzwerte aus den Trainingsdaten ab oder (3) eine Kombination der ersten beiden Arten.

### Typologie von Gesichtserkennungssystemen



Die technische Zuverlässigkeit von Gesichtserkennungssystemen hat in den vergangenen Jahren zugenommen. Unter idealen Bedingungen liegt die Zuverlässigkeit bestimmter Systeme bei bis zu 99,97 % (Crumpler 2020).

| | Detektion | Authentifikation | Identifikation | Klassifizierung |
|---|---|---|---|---|
| **Anwendungsbeispiele** | Grundlage für alle weiteren Gesichtserkennungstechnologien | Passkontrolle, Entsperren des Telefons | Polizei gleicht Videoausschnitt im Rahmen von Ermittlungsarbeit mit Datenbank ab | Altersfeststellung, Aufmerksamkeitskontrolle |
| **Antwort auf** | Ist auf dem Foto oder in dem Video ein Gesicht zu sehen? | Ist das die Person, für die sie sich ausgibt? | Wer ist die Person auf dem Foto? | Wie soll eine bestimmte Person klassifiziert werden? |
| **Potenzielle Vorteile** | Gesichter erkennen und zuordnen | Kostensenkung, besserer und einfacherer Identitätsnachweis | Effizientere Verfolgung von Straftaten | Müdigkeitsfeststellung im Kraftfahrzeug, verbesserte Diagnose von Krankheiten |
| **Potenzielle Nachteile** | Gesichter werden nicht erkannt oder falsch zugeordnet | Erhöhte Schwierigkeit, etwa eine Passkontrolle zu passieren | Fehlerquote: Unschuldige Person im Fokus der Ermittlungsbehörden | Falsche Klassifizierung: Betroffenen werden unzutreffenderweise Persönlichkeitsmerkmale zugeordnet |

Die technische Zuverlässigkeit hängt stark von der Qualität der Trainingsdaten ab. Je weniger divers oder je weniger repräsentativ ein Datensatz ist, desto höher ist die Wahrscheinlichkeit, dass eine Gruppe unterrepräsentiert ist und sie somit für den Algorithmus nicht oder nur schwer klassifizierbar ist. Auch veränderte Umweltbedingungen, wie verschwommene oder verpixelte Fotos und Videomaterial ohne Frontalansicht sowie Mund-Nase-Bedeckungen während der Coronapandemie, können sich auf die technische Zuverlässigkeit der Systeme auswirken (Ngan et al. 2020).

## 3. Rechtlicher Rahmen

Wenn Systeme technisch nicht zuverlässig sind, können sie nicht ohne Weiteres durch öffentliche Stellen Bürgerinnen und Bürgern gegenüber eingesetzt werden, denn der verfassungsrechtliche Grundsatz der Verhältnismäßigkeit gebietet es, dass die durch Behörden angewandten Mittel geeignet sein müssen, die verfolgten Zwecke der Authentifikation, Klassifizierung oder Identifikation zu erreichen. Es kann sich zudem die Frage der Angemessenheit stellen: Welcher Zweck einer Maßnahme rechtfertigt es, dass Bürgerinnen und Bürger falsch identifiziert und polizeilichen Maßnahmen unterworfen werden können?

Technische Unzuverlässigkeit kann ebenfalls bedeuten, dass die Systeme beispielsweise Menschen mit helleren und dunkleren Hauttypen oder Männer und Frauen nicht gleich behandeln und so gegen den Gleichheitssatz des Grundgesetzes verstoßen (Art. 3 Grundgesetz).

Auch zwischen Privaten muss Gesichtserkennungssoftware technisch zuverlässig sein. Dies dürfte im vertraglichen Bereich die im Verkehr erforderliche Sorgfalt bzw. im außervertraglichen Bereich die Verkehrssicherungspflicht gebieten. Andernfalls drohen Haftungsrisiken.

Selbst wenn die Systeme technisch zuverlässig sind, heißt das noch nicht, dass sie auch rechtlich zulässig sind. Wer immer Gesichtserkennungssoftware einsetzt, muss weitere verfassungsrechtliche und datenschutzrechtliche Anforderungen beachten.

Wenn öffentliche Stellen Gesichtserkennung einsetzen, greifen sie in das Recht auf informationelle Selbstbestimmung von Bürgerinnen und Bürgern ein. Das Grundrecht schützt betroffene Personen vor einer unbegrenzten Verarbeitung ihrer personenbezogenen Daten. Eingriffe sind nur zulässig, sofern die Betroffenen zustimmen oder es eine gesetzliche Grundlage für den Eingriff gibt. Die gesetzliche Ermächtigungsgrundlage muss verhältnismäßig sowie normenklar und bestimmt sein und auch technische und organisatorische Schutzvorkehrungen aufweisen (Bundesverfassungsgericht – Volkszählungsurteil).

Öffentliche und private Stellen haben zudem die Datenschutz-Grundverordnung sowie die Richtlinie für Justiz und Inneres, das Bundesdatenschutzgesetz sowie gegebenenfalls bereichsspezifische Normen zu beachten. Auch hier gilt: Eine Datenverarbeitung ist grundsätzlich verboten, es sei denn, die Betroffenen haben eingewilligt oder es gibt eine gesetzliche Grundlage für die Verarbeitung (Verbot mit Erlaubnisvorbehalt).

Wird Gesichtserkennung zum Zweck der Authentifikation oder der Identifikation eingesetzt, werden besonders sensible Kategorien personenbezogener Daten verarbeitet, nämlich biometrische Daten. Eine Verarbeitung ist nur mit ausdrücklicher Einwilligung oder unter engen gesetzlichen Voraussetzungen erlaubt (Art. 9 Datenschutz-Grundverordnung).

Bei einer Datenverarbeitung zu Zwecken der Klassifizierung handelt es sich nicht um biometrische Daten, wenn nicht die Identifikation einer Person bezweckt wird, sondern beispielsweise nur das Alter, das Geschlecht, die Aufmerksamkeit oder eine Krankheit gemessen werden soll. Allerdings kann es sich dann, je nach Fallkonstellation, ebenfalls um besonders sensible Kategorien personenbezogener Daten, etwa Gesundheitsdaten, handeln. Die Datenverarbeitung ist ebenfalls nur mit (ausdrücklicher) Einwilligung oder auf Basis einer (engen) gesetzlichen Grundlage zulässig (Art. 6 u. Art. 9 Datenschutz-Grundverordnung).

Bei der Datenverarbeitung sind datenschutzrechtliche Grundsätze einzuhalten, die in den Einzelvorschriften der datenschutzrechtlichen Gesetze konkretisiert werden und eine Ausprägung des Verhältnismäßigkeitsgrundsatzes darstellen (Art. 5 Datenschutz-Grundverordnung). Beim Einsatz von Gesichtserkennungssoftware ist zudem eine Datenschutzfolgenabschätzung durchzuführen, damit datenschutzrechtliche Vorschriften eingehalten werden (Art. 35 Datenschutz-Grundverordnung). Ein Schutz vor Fehlentscheidungen von Gesichtserkennungsprogrammen wird durch das Verbot automatisierter Einzelentscheidungen gewährleistet (Art. 22 Datenschutz-Grundverordnung). Betroffene müssen in jedem Fall die Möglichkeit haben, dass doch wieder ein Mensch die Entscheidung trifft, und nicht die Software.

# 4. Impulse zur Regulierung von Gesichtserkennung

## 4.1 Authentifikation

Die Anwendung von Gesichtserkennung zur Authentifizierung, beispielsweise zum Entsperren des Mobiltelefons oder zur Passkontrolle, ist zulässig, wenn die datenschutzrechtlichen Grundsätze bzw. die sie konkretisierenden Vorschriften der Datenschutz-Grundverordnung, des Bundesdatenschutzgesetzes sowie gegebenenfalls bereichsspezifischer Normen eingehalten werden. Die Authentifikation wird durch die bestehenden datenschutzrechtlichen Normen ausreichend geregelt.

### Bewertung

Ein gesetzgeberischer Handlungsbedarf ist nicht gegeben.

## 4.2 Klassifizierung

Um Diskriminierung von Betroffenen zu verhindern, fordert der Europarat in seinen Regulierungsvorschlägen vom 28. Januar 2021, dass bestimmte Gesichtserkennungssysteme verboten werden sollen. Gesichtserkennung, deren einziges Ziel es ist, die Hautfarbe, die religiöse oder sonstige Überzeugung, das Geschlecht, die ethnische Herkunft, das Alter oder den gesundheitlichen bzw. sozialen Zustand einer Person zu bestimmen, solle verboten werden (Council of Europe 2021a, 2021b).

Ebenfalls verboten werden sollen „Affekt-Erkennungstechnologien“, die Emotionen erkennen und dazu benutzt werden können, Persönlichkeitsmerkmale, innere Gefühlszustände, die psychische Gesundheit oder den Grad des Engagements von Arbeitnehmerinnen und Arbeitnehmern zu bestimmen. Diese Form der Technologie stelle ein hohes Risiko dar, etwa bei Beschäftigungsverhältnissen, beim Zugang zu Versicherungen und zu einer Ausbildung (Council of Europe 2021a, 2021b).

Ähnlich empfehlen der Europäische Datenschutzausschuss und der Europäische Datenschutzbeauftragte in einer gemeinsamen Stellungnahme vom 18. Juni 2021, dass Künstliche Intelligenz wie Gesichtserkennung verboten werden solle, die Individuen kategorisieren kann: nach ihrer ethnischen Herkunft, ihrem Geschlecht, ihrer politischen oder sexuellen Orientierung oder aus anderen nach Artikel 21 der Europäischen Grundrechtecharta verbotenen diskriminierenden Gründen (European Data Protection Board, European Data Protection Supervisor 2021). Gleichfalls solle Künstliche Intelligenz verboten werden, die Emotionen von Betroffenen erkennen kann, mit Ausnahme im Bereich Gesundheit und Forschung (European Data Protection Board, European Data Protection Supervisor 2021).

Anders als der Europarat schlägt die Europäische Kommission in ihren Regulierungsvorschlägen zu Künstlicher Intelligenz nicht vor, diese Formen von Gesichtserkennung zu verbieten. Als „System zur biometrischen Kategorisierung“ bzw. „Emotionserkennungssystem“ sollen für die Systeme allerdings spezifische Transparenzverpflichtungen gelten (Art. 52 Entwurf KI-Verordnung, EU-Kommission 2021a).

Auch können die Systeme in den Bereichen „Allgemeine und berufliche Bildung“, „Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit“, „Zugänglichkeit und Inanspruchnahme grundlegender privater und öffentlicher Dienste und Leistungen“, „Strafverfolgung“ sowie „Migration, Asyl und Grenzkontrolle“ als Künstliche Intelligenz mit hohem Risiko eingestuft und weiteren strikten obligatorischen Auflagen unterworfen werden (Anhang III zu Entwurf KI-Verordnung, EU-Kommission 2021b).

## Bewertung

Die vom Europarat und der Europäischen Kommission adressierten Formen der Gesichtserkennung sind bereits verboten, es sei denn, die Betroffenen willigen in die Klassifizierung ein (datenschutzrechtliches Verbot mit Erlaubnisvorbehalt). Denn eine gesetzliche Rechtsgrundlage, die – ohne das Einverständnis der Betroffenen – zum Einsatz der Systeme berechtigte, ist nicht ersichtlich und dürfte nicht geschaffen werden können, da sie unverhältnismäßig wäre.

Die für die Klassifizierung erforderliche Einwilligung muss freiwillig sein, sodass in Fällen eines Ungleichgewichts der Macht, wie zwischen Behörden und Bürgerinnen bzw. Bürgern sowie Arbeitgeberinnen bzw. Arbeitgebern und Arbeitnehmerinnen bzw. Arbeitnehmern, eine Einwilligung regelmäßig nicht in Betracht kommt.

Es verbleibt eine eng begrenzte Anzahl von Fällen, in denen eine Klassifizierung durch Gesichtserkennungssysteme auf Basis einer freiwilligen Einwilligung der Betroffenen zulässig sein kann. Dies sind insbesondere die Bereiche Gesundheit, Wissenschaft und Sicherheit des Straßenverkehrs.

Auf Grundlage einer freiwilligen Einwilligung können also enge Anwendungsfälle durchgeführt werden, etwa das Erkennen von Krankheiten, die Kontrolle der Aufmerksamkeit von Kraftfahrzeugführern oder wissenschaftliche Forschung.

In den verbleibenden denkbaren Fällen gewährleistet die freiwillige Einwilligung die Autonomie der Betroffenen über ihre personenbezogenen Daten und sie können sich dem Risiko einer Diskriminierung auf diesem Wege erst gar nicht aussetzen.

Selbst wenn sie ausdrücklich, freiwillig und informiert einwilligen, so müssen sie nach dem Verbot automatisierter Einzelentscheidungen stets die Möglichkeit haben, dass doch wieder ein Mensch die Entscheidung inhaltlich verantwortet und ihren Standpunkt berücksichtigt. Dies wirkt einer Diskriminierung durch fehlerhafte Gesichtserkennungstechnologie entgegen, die etwa durch nicht repräsentative Datensätze entstehen kann.

Vor diesem Hintergrund scheint der geltende datenschutzrechtliche Rechtsrahmen in einem Maße Schutz vor Diskriminierung zu bieten, dass ein vom Europarat und den europäischen Datenschutzaufsichtsbehörden vorgeschlagenes ausdrückliches gesetzliches Verbot (mit engen Ausnahmen) dieser Form der Technologie nicht notwendig sein dürfte.

Aus Gründen der Rechtssicherheit sollten die Europäischen Datenschutzaufsichtsbehörden jedoch in einer gemeinsamen Stellungnahme die bestehenden engen Anwendungsfälle des Einsatzes der Systeme zum Zwecke der Klassifikation festlegen.

Es erscheint in jedem Fall zielführend, den gesetzlichen Schutz vor Diskriminierung zu verstärken, wie es die Europäische Kommission mit ihren Regulierungsvorschlägen anstrebt. In den sensiblen Bereichen „Allgemeine und berufliche Bildung“, „Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit“, „Zugänglichkeit und Inanspruchnahme grundlegender privater und öffentlicher Dienste und Leistungen“, „Strafverfolgung“ sowie „Migration, Asyl und Grenzkontrolle“ sollte diese Form von Technologie als Künstliche Intelligenz mit hohem Risiko gelten und einer vorab vorzunehmenden Konformitätsbewertung und obligatorischen Auflagen unterworfen werden.

Gleichwohl sind all dies Bereiche, in denen ein Einsatz von Gesichtserkennungssoftware zur Klassifizierung auf Basis einer freiwilligen Einwilligung infolge eines bestehenden Machtungleichgewichts regelmäßig nicht in Betracht kommen dürfte und demnach verboten ist (datenschutzrechtliches Verbot mit Erlaubnisvorbehalt).

Die Europäische Kommission sollte den Bereich „Gesundheit“ in ihren Katalog von Künstlicher Intelligenz (KI) mit hohem Risiko aufnehmen. Denn gerade im Gesundheitskontext scheint eine Anwendung von Gesichtserkennungssystemen auf Basis einer freiwilligen Einwilligung denkbar. Hier sollten fälschliche Diagnosen vermieden werden, indem die Systeme den „Hochrisiko-KI-Auflagen“ unterworfen werden, sodass sie insbesondere mit repräsentativen Datensätzen trainiert, menschlich beaufsichtigt und genau sind.

## 4.3 Identifikation

### a) Clearview und PimEyes

Clearview ist ein US-amerikanisches Unternehmen mit Sitz in New York, das eine Datenbank von mehr als drei Milliarden Aufnahmen von Gesichtern angelegt hat. Diese wurden aus dem Internet zusammengesucht, insbesondere aus sozialen Netzwerken oder von Unternehmensseiten. Kundinnen und Kunden können mittels einer Gesichtserkennungssoftware ein Foto mit den gespeicherten Milliarden von Aufnahmen abgleichen. Es werden dann Suchergebnisse mit Fotos angezeigt, einschließlich der Quelle, beispielsweise von einer Unternehmensseite oder aus einem sozialen Netzwerk (Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit 2020). Genutzt wurde Clearview insbesondere von Sicherheitsbehörden, die mithilfe der Gesichtserkennungssoftware Verdächtige identifizierten (Laufer 2020).

PimEyes ist ein Unternehmen mit ehemals Sitz in Polen, jetzt auf den Seychellen, das ebenso wie Clearview die Identifikation von Personen mittels Gesichtserkennungssoftware anbietet. Der Unterschied zu Clearview: Die Datenbank ist „kleiner" – sie umfasst etwa 900 Millionen Menschen – und der Service wird für jedermann, also nicht nur für Sicherheitsbehörden, angeboten (Dachwitz et al. 2020).

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit hat nach einer Beschwerde ein Verfahren gegen Clearview eröffnet, die Anwendbarkeit der Datenschutz-Grundverordnung bejaht, die Rechtswidrigkeit der Verarbeitung des Hashwertes des Fotos des Beschwerdeführers festgestellt und angeordnet, dass der Hashwert des Fotos des Beschwerdeführers zu löschen ist. Kritisiert wurde daraufhin insbesondere,

dass kein europaweites Verbot von Clearview ausgesprochen, sondern nur der einzelne Beschwerdefall behandelt wurde. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit hat diesbezüglich mitgeteilt, dass eine solche Anordnung nicht umzusetzen sei. Denn es sei nicht davon auszugehen, dass Clearview Informationen über den gewöhnlichen Wohnort der Betroffenen (in Hamburg) habe (Beuth 2021).

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg hat ein Verfahren gegen PimEyes eröffnet. Das Unternehmen hat seinen Fragenkatalog aber bislang nicht beantwortet (Kurz 2021).

## Bewertung

Nach geltendem Recht ist die Verarbeitung biometrischer Daten von Bürgerinnen und Bürgern der Europäischen Union durch Clearview und PimEyes verboten. Die Betroffenen haben regelmäßig nicht eingewilligt und eine gesetzliche Rechtsgrundlage für die Verarbeitung ist nicht ersichtlich (datenschutzrechtliches Verbot mit Erlaubnisvorbehalt).

Gleichwohl zeigt sich am Beispiel Clearview und PimEyes, dass ein Problem der Durchsetzung des geltenden Rechts gegenüber Unternehmen im Ausland zu bestehen scheint.

Hintergrund dürfte zum einen sein, dass eine Anordnung auf Löschung aller personenbezogenen Daten von EU-Bürgerinnen und -Bürgern daran scheitert, dass die Unternehmen nicht feststellen können, wer auf den gespeicherten Fotos Unionsbürgerin oder Unionsbürger ist. Zum anderen scheinen die Unternehmen mit Sitz im Drittland den Ersuchen der Aufsichtsbehörden nicht zuverlässig nachzukommen.

Hier ist der Gesetzgeber gefragt, gemeinsam mit den Datenschutzaufsichtsbehörden über Wege und Mittel zur Durchsetzung des geltenden Rechts zu beraten.

Gegebenenfalls bedarf es völkerrechtlicher Verträge der EU mit Drittstaaten, um die personenbezogenen Daten von EU-Bürgerinnen und -Bürgern zu schützen.

### b) Biometrische Gesichtserkennung im öffentlichen Raum

Bekannt ist die biometrische Gesichtserkennung vor allem durch den Test am Bahnhof Berlin Südkreuz in den Jahren 2017 und 2018. Mit der Technik werden alle Bürgerinnen und Bürger im Anwendungsfeld der Videokameras mit biometrischer Gesichtserkennung „live" gescannt und mit einer Datenbank der Ermittlungsbehörden abgeglichen.

Im Unterschied zu Clearview und PimEyes soll diese Gesichtserkennung räumlich begrenzt eingesetzt werden, etwa an Bahnhöfen, und es soll eine konkrete Datenbank von Verdächtigen durchsucht werden.

Über die Zulassung und den Einsatz dieser Technik im öffentlichen Raum gibt es europäische und nationale Regulierungsbestrebungen.

Die EU-Kommission hat zunächst ein Verbot dieser Form von Gesichtserkennung im öffentlichen Raum für die nächsten fünf Jahre erwogen (Fanta 2020). In ihrem im Februar 2020 veröffentlichten *Weißbuch Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen* rückte sie davon jedoch ab. Sie schlug lediglich vor, dass die Technik „ausnahmslos als mit hohem Risiko behaftet angesehen" und obligatorischen strikten Auflagen unterworfen werden solle, die in einer vorab vorzunehmenden Konformitäts-

bewertung überprüft und kontinuierlich überwacht werden sollen. Die KI-Anwendung soll als mit einem hohen Risiko behaftet angesehen werden, da sie besondere Risiken in Bezug auf die Achtung der Grundrechte birgt, insbesondere für die Achtung des Privatlebens und den Schutz personenbezogener Daten sowie im Bereich der Nichtdiskriminierung (EU-Kommission 2020).

In ihren am 21. April 2021 veröffentlichten Regulierungsvorschlägen zu Künstlicher Intelligenz geht die Europäische Kommission nun einen Mittelweg (EU-Kommission 2021a): Die Technik soll grundsätzlich verboten und nur ausnahmsweise erlaubt sein.

Danach soll die Verwendung von Echtzeit-Fernidentifizierungssystemen in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken verboten sein, außer wenn und insoweit dies im Hinblick auf eines der folgenden Ziele unbedingt erforderlich ist:

- Gezielte Suche nach bestimmten potenziellen Opfern von Straftaten oder nach vermissten Kindern

- Abwenden einer konkreten, erheblichen und unmittelbaren Gefahr für das Leben oder die körperliche Unversehrtheit natürlicher Personen oder eines Terroranschlags

- Erkennen, Aufspüren, Identifizieren oder Verfolgen eines Täters oder Verdächtigen einer Straftat im Sinne des Artikel 2 Absatz 2 des Rahmenbeschlusses 2002/584/JI des Rates, der in dem betreffenden Mitgliedstaat nach dessen Recht mit einer Freiheitsstrafe oder einer freiheitsentziehenden Maßregel der Sicherung im Höchstmaß von mindestens drei Jahren bedroht ist (Art. 5 Abs. 1 lit. d) Entwurf KI-Verordnung, EU-Kommission 2021a).

Wenn die biometrische Gesichtserkennung im öffentlichen Raum für einen der oben genannten Gründe eingesetzt wird, soll auf der einen Seite die Art der Situation berücksichtigt werden, die der möglichen Verwendung zugrunde liegt, insbesondere wie schwer der Schaden wiegen würde, wie wahrscheinlich er wäre und in welchem Ausmaß er aufträte, wenn das System nicht eingesetzt würde. Auf der anderen Seite sollen die Folgen für die Rechte und Freiheiten aller betroffenen Personen berücksichtigt werden, wenn das System eingesetzt wird, insbesondere wie schwer und wahrscheinlich die Folgen sind und in welchem Ausmaß sie auftreten (Art. 5 Abs. 2 Entwurf KI-Verordnung, EU-Kommission 2021a). Hier sieht die Europäische Kommission eine Güterabwägung zwischen den Folgen des Einsatzes und den Folgen des Nichteinsatzes von biometrischer Gesichtserkennung im öffentlichen Raum vor.

Auch soll die Anwendung von biometrischer Gesichtserkennung im öffentlichen Raum von notwendigen und angemessenen Schutzvorkehrungen begleitet sein, insbesondere in Bezug auf deren zeitliche, räumliche und personenbezogene Beschränkungen (Art. 5 Abs. 2 Entwurf KI-Verordnung, EU-Kommission 2021a).

Jede Anwendung von biometrischer Gesichtserkennung im öffentlichen Raum soll durch eine Justizbehörde oder eine andere unabhängige Verwaltungsbehörde genehmigt werden. In begründeten dringenden Fällen soll die Anwendung auch ohne eine solche Genehmigung begonnen werden können. Die Genehmigung soll in diesem Fall nachgeholt werden.

Die genehmigende Stelle soll biometrische Gesichtserkennung im öffentlichen Raum nur erlauben, wenn sie auf der Grundlage objektiver Nachweise oder eindeutiger Hinweise davon überzeugt ist, dass der Einsatz notwendig und verhältnismäßig ist, um einen der oben genannten Gründe zu

erreichen; dabei soll die genannte Güterabwägung zwischen den Folgen des Einsatzes und des Nichteinsatzes stattfinden (Art. 5 Abs. 3 Entwurf KI-Verordnung, EU-Kommission 2021a).

Ein Mitgliedstaat soll entscheiden dürfen, biometrische Gesichtserkennung in öffentlich zugänglichen Räumen in seinem nationalen Recht ganz oder teilweise innerhalb der oben genannten Grenzen und unter diesen Bedingungen zu erlauben. Der Mitgliedstaat soll dazu in seinem nationalen Recht die notwendigen detaillierten Regeln erlassen (Art. 5 Abs. 4 Entwurf KI-Verordnung, EU-Kommission 2021a). Die EU-Kommission gibt insofern lediglich einen Rahmen vor, innerhalb dessen der nationale Gesetzgeber eine Rechtsgrundlage schaffen kann.

Auch soll biometrische Gesichtserkennung im öffentlichen Raum als eine Technologie mit hohem Risiko eingestuft werden, für die obligatorische Auflagen gelten, die in einem Konformitätsbewertungsverfahren geprüft und laufend überwacht werden (Anhang III zu Entwurf KI-Verordnung, EU-Kommission 2021b).

Ob die Regulierungsvorschläge der Europäischen Kommission Gesetz werden, ist noch offen. Dazu müsste das Europäische Parlament und der Rat der Europäischen Union zustimmen, da die Vorschläge im ordentlichen Gesetzgebungsverfahren beschlossen werden (EUR-Lex 2021).

Derzeit spricht sich das Europäische Parlament in einer Entschließung vom 6. Oktober 2021 für ein Verbot von biometrischer Gesichtserkennung im öffentlichen Raum aus und fordert die Europäische Kommission auf, „mit legislativen und nichtlegislativen Mitteln und erforderlichenfalls durch Vertragsverletzungsverfahren ein Verbot jeglicher Verarbeitung biometrischer Daten, einschließlich Gesichtsbildern, zu Strafverfolgungszwecken

zu erwirken, wenn diese Verarbeitung zu einer Massenüberwachung in öffentlich zugänglichen Räumen führt." (Europäisches Parlament 2021).

Dem schließen sich die Parteien der Ampel-Regierung im Koalitionsvertrag an: Sie wollen die biometrische Erkennung im öffentlichen Raum europarechtlich ausschließen (SPD/Die Grünen/FDP 2021).

Auch der Europäische Datenschutzausschuss und der Europäische Datenschutzbeauftragte empfehlen in einer gemeinsamen Stellungnahme vom 18. Juni 2021, dass die biometrische Gesichtserkennung im öffentlichen Raum gänzlich verboten werden solle. Insbesondere habe die Technik unumkehrbare und schwere Auswirkungen auf die (vernünftige) Erwartung der Bevölkerung, sich anonym in der Öffentlichkeit zu bewegen. Dies habe auch negative Effekte auf die Ausübung von Meinungsfreiheit, Versammlungsfreiheit und Bewegungsfreiheit (European Data Protection Board, European Data Protection Supervisor 2021).

Sollte das Europäische Parlament aber nicht bei seiner Haltung bleiben oder sollte sich die Ampel-Regierung nicht im Rat der Europäischen Union durchsetzen können, und die EU über kurz oder lang einen Rahmen für die Technologie vorgeben, so könnte der deutsche Gesetzgeber innerhalb dieses Rahmens eine Rechtsgrundlage für die biometrische Gesichtserkennung im öffentlichen Raum schaffen.

Bestrebungen, eine nationale Rechtsgrundlage für den Einsatz von biometrischer Gesichtserkennung im öffentlichen Raum in Deutschland zu schaffen, wurden wieder aufgegeben. Im Entwurf des neuen Bundespolizeigesetzes hieß es zum Jahresbeginn 2020, dass die Bundespolizei Daten aus Bildaufzeichnungsgeräten „automatisch mit biometrischen Daten abglei-

chen“ könne. Aus dem späteren Entwurf wurde dieser Passus gestrichen (Spiegel-Meldung 2020).

Es ist insofern umstritten, ob es derzeit eine Rechtsgrundlage für den Einsatz der Systeme gibt. Ebenfalls umstritten ist, ob eine Rechtsgrundlage geschaffen werden könnte, die den verfassungsrechtlichen Anforderungen genügt.

### Bewertung

Derzeit ist keine Ermächtigungsgrundlage für die biometrische Gesichtserkennung auf Bundesebene ersichtlich. Bestehende Rechtsgrundlagen sind angesichts der Schwere des Grundrechtseingriffs nach der Rechtsprechung des Bundesverfassungsgerichts nicht bestimmt und normenklar genug, um die Technik zu erlauben. Denn je schwerer ein Grundrechtseingriff wiegt, desto höher sind die Anforderungen an die Klarheit und Bestimmtheit einer Ermächtigungsgrundlage (Bundesverfassungsgericht – Kennzeichen I). Bestehende Rechtsgrundlagen normieren lediglich Bildaufnahmen bzw. Bildaufzeichnungen.

Mangels Rechtsgrundlage ist die Technologie damit derzeit auf Bundesebene verboten (datenschutzrechtliches Verbot mit Erlaubnisvorbehalt).

Bei der Frage, ob der Gesetzgeber biometrische Gesichtserkennung im öffentlichen Raum erlauben dürfte, lässt sich insbesondere die Rechtsprechung des Bundesverfassungsgerichts zur Kfz-Kennzeichen-Kontrolle heranziehen (Bundesverfassungsgericht – Kennzeichen I und Kennzeichen II). Den Urteilen lag der Fall zugrunde, dass Kfz-Kennzeichen mit einer Videokamera optisch erfasst, mittels einer Software ausgelesen und mit polizeilichen Fahndungsdatenbanken abgeglichen wurden, sodass Parallelen zur biometrischen Gesichtserkennung bestehen. Gleichwohl handelt es sich

bei biometrischer Gesichtserkennung im öffentlichen Raum um eine eingriffsintensivere Maßnahme, da das höchstpersönliche Merkmal Gesicht erfasst würde, sodass deutlich höhere verfassungsrechtliche Hürden als bei der Kfz-Kennzeichen-Kontrolle gelten dürften.

So dürfte die Eingriffsintensität der biometrischen Gesichtserkennung im öffentlichen Raum näher an der „Rasterfahndung" (Bundesverfassungsgericht – Rasterfahndung) und der „Online-Durchsuchung" (Bundesverfassungsgericht – Online-Durchsuchung) liegen. Darum ist ebenfalls die Rechtsprechung des Bundesverfassungsgerichts zu diesen Fahndungsmaßnahmen heranzuziehen. Die Rasterfahndung bietet sich als Vergleich an, da bei ihr ebenfalls eine Vielzahl von völlig unauffälligen Personen „gescannt" wird. Die Online-Durchsuchung ist wohl vergleichbar, da bei ihr gleichfalls höchstpersönliche Merkmale der Persönlichkeit von Betroffenen bei der Fahndung betroffen sind.

Da die Maßnahme eine hohe Anzahl von Bürgerinnen und Bürgern erfasst, die keinen Anlass dafür gegeben haben, und dadurch Einschüchterungseffekte („chilling effects") entstehen, liegt ein schwerer Grundrechtseingriff vor. Der Gesetzgeber dürfte darum wohl nur innerhalb sehr enger verfassungsrechtlicher Grenzen eine Ermächtigungsgrundlage für eine Videoüberwachung mittels biometrischer Gesichtserkennung schaffen und die Technik erlauben.

Die verfassungsrechtlichen Grenzen sind wohl noch enger als der enge Rahmen, den die Europäische Kommission in ihren Regulierungsvorschlägen anstrebt:

- Dem Rahmen der Europäische Kommission zufolge darf biometrische Gesichtserkennung an „öffentlich zugänglichen Räumen“ durch den nationalen Gesetzgeber erlaubt werden. Dies umfasst „einen der Öffentlichkeit zugänglichen Ort, unabhängig davon, ob sich der betreffende Ort in privatem oder öffentlichem Eigentum befindet [...] Folglich sind neben öffentlichen Straßen, relevanten Teilen von Regierungsbehörden und den meisten Verkehrsinfrastrukturen auch Bereiche wie Kinos, Theater, Geschäfte und Einkaufszentren in der Regel öffentlich zugänglich.“ (Erwägungsgrund 9 zu Entwurf KI-Verordnung, EU-Kommission 2021a).

  Aufgrund der Schwere der Maßnahme, insbesondere ihrer Einschüchterungseffekte, dürfte verfassungsrechtlich biometrische Gesichtserkennung nur an eng bestimmten öffentlich zugänglichen Räumen wie Verkehrsknotenpunkten, beispielsweise Bahnhöfen oder Flughäfen, zulässig sein. Ein Einsatz der Technologie an sämtlichen öffentlich zugänglichen Orten, wie in Einkaufszentren, Kinos, Theatern, Geschäften oder Fußgängerzonen sowie sämtlichen übrigen Verkehrsinfrastrukturen, ist verfassungsrechtlich wohl nicht zu halten und dürfte durch den nationalen Gesetzgeber nicht erlaubt werden.

- Nach den Vorschlägen der EU-Kommission soll die biometrische Gesichtserkennung zulässig sein zur Aufklärung von Straftaten, die in Artikel 2 Abs. 2 des Rahmenbeschlusses des Rates vom 13. Juni 2002 über den Europäischen Haftbefehl und die Übergabeverfahren zwischen den Mitgliedstaaten genannt sind und die nach nationalem Recht mit einer Freiheitsstrafe oder einer freiheitsentziehenden Maßnahme der Sicherung im Höchstmaß von mindestens drei Jahren bedroht sind. Danach wären beispielsweise der Betrug (§ 263 Abs. 1

StGB) oder die Produktpiraterie (§ 143 Abs. 1 MarkenG) hiervon umfasst und könnten die biometrische Gesichtserkennung im öffentlichen Raum rechtfertigen.

Dies ist verfassungsrechtlich wohl unverhältnismäßig. Aufgrund der Vergleichbarkeit der Eingriffstiefe der biometrischen Gesichtserkennung im öffentlichen Raum mit der „Online-Durchsuchung" dürfte die Technologie verfassungsrechtlich ebenfalls nur zur Aufklärung besonders schwerer Straftaten (§ 100b StPO) durch den nationalen Gesetzgeber erlaubt werden.

- Die Verfassung gibt enge organisatorische und verfahrensrechtliche Schutzvorkehrungen vor, die in einer nationalen Rechtsgrundlage berücksichtigt werden müssen. Dazu gehört nicht allein der von der Europäischen Kommission vorgesehene Richtervorbehalt, sondern auch die Beteiligung des Bundesbeauftragten für den Datenschutz, Informations-, Auskunfts-, Lösch- und Verwendungsbegrenzungspflichten sowie ein hohes Maß an Datensicherheit.

- Verfassungsrechtlich ist zudem eine „doppelte Verhältnismäßigkeitsprüfung" mittels einer Überwachungs-Gesamtrechnung erforderlich.

Auch wenn der Gesetzgeber wohl eine Ermächtigungsgrundlage innerhalb sehr enger verfassungsrechtlicher Grenzen schaffen dürfte, so sollte er dies nur tun, wenn die Gesellschaft die Technologie auch will, also akzeptiert. Die Frage der gesellschaftlichen Akzeptanz scheint jedoch noch nicht geklärt zu sein.

Nach einer Studie der Freien Universität Berlin und der Universität St. Gallen im Jahr 2020 zur Akzeptanz von Gesichtserkennungstechnologie in der Bevölkerung waren im Hinblick auf biometrische Gesichtserkennung im öffentlichen Raum in Deutschland 39 % der Befragten gegen den Einsatz (davon 18 % stark dagegen, 21 % dagegen), 37 % akzeptierten die Technik (davon 8 % stark dafür, 29 % dafür) und 24 % waren weder dagegen noch dafür (Steinacker et al. 2020).

Dies spricht dafür, dass eine weitergehende breite öffentliche demokratische Debatte über den Einsatz der Technologie erforderlich sein dürfte. Insofern ist es zu begrüßen, dass die Europäische Kommission in ihrem *Weißbuch zur Künstlichen Intelligenz* eine „breit angelegte europäische Debatte über die besonderen Umstände, die eine solche Nutzung rechtfertigen könnten, sowie über gemeinsame Sicherheitsvorkehrungen" angekündigt hat (EU-Kommission 2020).

Sollten die Regulierungsvorschläge der EU-Kommission Gesetz werden, könnte der deutsche Gesetzgeber innerhalb des vorgegebenen europäischen Rahmens eine Rechtsgrundlage schaffen. Davon sollte er aber absehen bis eine demokratische Debatte über die Technologie abgeschlossen ist („Moratorium").

### c) Gesichtserkennung beim G20-Gipfel in Hamburg

Die Polizei Hamburg hat zur Aufklärung von Straftaten anlässlich des G20-Gipfels Gesichtserkennungssysteme angewandt, um Tausende (auch) unbeteiligte Personen auf Bild- und Videoaufnahmen zu detektieren (1. Schritt) und später einen Abgleich mit anderen Dateien durchzuführen, um Straftäter zu identifizieren (2. Schritt).

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit hat das Verfahren der Polizei Hamburg beanstandet und später eine Löschung der gespeicherten Daten angeordnet. Er stützt seine Beanstandung insbesondere darauf, dass die Generalklausel, die die Polizei Hamburg ihrer Maßnahme zugrunde gelegt hat, nach der Rechtsprechung des Bundesverfassungsgerichts für einen so schweren Grundrechtseingriff zu unbestimmt sei (Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit 2019). Denn je schwerer ein Grundrechtseingriff, desto höher die Anforderungen an die Bestimmtheit der Ermächtigungsgrundlage. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit verweist dabei insbesondere auf die Rechtsprechung des Bundesverfassungsgerichts zur Videoüberwachung von öffentlichen Plätzen. Danach ist eine datenschutzrechtliche Generalklausel zur Videoüberwachung als zu unbestimmt für einen Eingriff in die Grundrechte von einer großen Anzahl von Personen anzusehen, wenn die Personen durch ihr Verhalten keinen Anlass zu einer Überwachung gegeben haben (Bundesverfassungsgericht – Videoüberwachung an öffentlichen Plätzen).

Dagegen hat die Polizei Hamburg geklagt und vor dem Verwaltungsgericht Hamburg recht bekommen (Verwaltungsgericht Hamburg). Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit hat die Zulassung der Berufung beantragt, der Fall ist somit ober- und höchstgerichtlich noch nicht entschieden.

## Bewertung

Die Ansicht des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit ist nach der Rechtsprechung des Bundesverfassungsgerichts zur Normenklarheit und Bestimmtheit von Ermächtigungsgrundlagen nachvollziehbar. Über eine solch wesentliche Frage, wie den Einsatz von Gesichtserkennungssoftware zur Aufklärung von Straftaten im Nachgang zu Massenereignissen, die eine große Anzahl auch Unbeteiligter betrifft, sollte der Gesetzgeber entscheiden. Eine Generalklausel dürfte hierfür nicht hinreichend bestimmt und normenklar sein. Der Gesetzgeber sollte für weitere vergleichbare Fälle in der Zukunft eine Spezialrechtsgrundlage zur Anwendung von Gesichtserkennung in der Strafprozessordnung normieren oder die Exekutive auf deren Einsatz verzichten.

### d) Gesichtserkennung durch die Polizei des Bundes und der Länder

Ein letzter Fall des Einsatzes von Gesichtserkennungssystemen ist der polizeiliche Abgleich von auf Video aufgenommenen Tatverdächtigen mit einer Datenbank des Bundeskriminalamts, um diese zu identifizieren. Im Unterschied zur biometrischen Gesichtserkennung im öffentlichen Raum findet kein „Live-Scannen“ von Personen statt, sondern es handelt sich um gespeicherte Videoaufzeichnungen. Der Unterschied zur biometrischen Gesichtserkennung im öffentlichen Raum und zum G20-Fall liegt zudem darin, dass ein biometrischer Abgleich nur mit Tatverdächtigen, nicht mit Unverdächtigen, durchgeführt wird. Gegen ein solches Verfahren bestehen keine grundsätzlichen datenschutzrechtlichen Bedenken, es wird aufgrund eines bestehenden Tatverdachts gegen eine Person ein Abgleich mit gespeicherten Bilddateien durchgeführt. Rechtsgrundlage für einen solchen Abgleich dürfte § 98c StPO sein.

### Bewertung

Gesetzgeberischer Handlungsbedarf ist nicht ersichtlich.

# 5. Fazit

1. Die technische Zuverlässigkeit von Gesichtserkennungssystemen nimmt zu. Doch selbst wenn die Technik zu 100 % technisch zuverlässig wäre, würde das nicht bedeuten, dass sie auch rechtlich zulässig ist.

   Neben der technischen Zuverlässigkeit der Systeme müssen weitere verfassungsrechtliche und datenschutzrechtliche Anforderungen eingehalten werden.

2. Der Einsatz von Gesichtserkennungssystemen zum Zwecke der Authentifikation kann datenschutzgerecht ausgestaltet werden. Regulierungsbedarf besteht nicht.

3. Klassifizierungen mittels Gesichtserkennungssystemen sind verboten, es sei denn, die Betroffenen willigen ein (datenschutzrechtliches Verbot mit Erlaubnisvorbehalt). Der Einsatz der Systeme ist nur in engen Anwendungsfällen auf Basis einer freiwilligen Einwilligung zulässig, insbesondere in den Bereichen Gesundheit, Wissenschaft und Sicherheit des Straßenverkehrs.

   Aus Gründen der Rechtssicherheit sollten die Europäischen Datenschutzaufsichtsbehörden in einer gemeinsamen Stellungnahme die engen Anwendungsfälle festlegen.

   Die Einwilligung muss freiwillig erfolgen, d. h. Betroffene dürfen sich nicht gedrängt fühlen oder negative Auswirkungen erdulden müssen, wenn sie nicht einwilligen. Mit ihrer freiwilligen Einwilligung können betroffene Personen Risiken von Diskriminierung durch Ge-

sichtserkennungssysteme im Vorfeld begegnen. Auch das Verbot automatisierter Einzelentscheidungen mindert Risiken von Diskriminierungen durch Gesichtserkennungssysteme, da die Betroffenen die Möglichkeit haben müssen, dass doch wieder ein Mensch die Entscheidung trifft.

Die Europäische Kommission sollte in ihren Regulierungsvorschlägen zu Künstlicher Intelligenz Klassifizierungen durch biometrische Systeme im Gesundheitsbereich als mit hohem Risiko behaftet ansehen und strikten obligatorischen Auflagen unterwerfen, da durch Fehldiagnosen erhebliche Nachteile für die Betroffenen entstehen können.

4. Der Einsatz von Gesichtserkennungssystemen zum Zwecke der Identifikation von Unionsbürgerinnen und Unionsbürgern durch private Unternehmen wie Clearview und PimEyes ist verboten, da die Betroffenen regelmäßig keine Einwilligung in die Verarbeitung ihrer biometrischen Daten gegeben haben. Es scheint jedoch ein Rechtsdurchsetzungsproblem zu geben.

   Um biometrische Daten zu schützen, sollte der Gesetzgeber mit den Datenschutzaufsichtsbehörden gemeinsam Lösungen erarbeiten. Gegebenenfalls bedarf es völkerrechtlicher Verträge der EU mit Drittstaaten.

5. Der Einsatz von Gesichtserkennungssystemen zum Zwecke der Identifikation im öffentlichen Raum ist derzeit mangels Rechtsgrundlage verboten (datenschutzrechtliches Verbot mit Erlaubnisvorbehalt).

   Der Staat hat eine Schutzpflicht für seine Bevölkerung, muss aber zugleich auch die Grundrechte seiner Bürgerinnen und Bürger achten.

Die Europäische Kommission will darum einen engen Rahmen vorgeben, in dem biometrische Gesichtserkennung im öffentlichen Raum ausnahmsweise zulässig sein soll. Ob sich die Regulierungsvorschläge der EU-Kommission im Europaparlament und dem Rat der Europäischen Union durchsetzen werden, ist derzeit noch offen.

Innerhalb des engen Rahmens könnte der nationale Gesetzgeber eine Rechtsgrundlage für die biometrische Gesichtserkennung im öffentlichen Raum schaffen.

Eine Rechtsgrundlage für die biometrische Gesichtserkennung im öffentlichen Raum muss den Grundsatz der Verhältnismäßigkeit beachten. Dabei ist eine doppelte Verhältnismäßigkeitsprüfung durchzuführen, die sowohl die Einzelmaßnahme als auch die Gesamtheit aller staatlichen Überwachungsinstrumente („Überwachungs-Gesamtrechnung“) berücksichtigt.

Im Hinblick auf die Überwachungs-Gesamtrechnung sollte wissenschaftliche Expertise eingeholt werden; das Gebiet wird derzeit beforscht.

Die biometrische Gesichtserkennung im öffentlichen Raum bedeutet einen sehr schweren Eingriff in die Grundrechte der Bürgerinnen und Bürger. Sie wäre wohl nur unter noch engeren verfassungsrechtlichen Voraussetzungen zulässig als dem bereits engen Rahmen, den die Europäische Kommission in ihren Regulierungsvorschlägen zu Künstlicher Intelligenz vorgeben will.

Zu den sehr engen verfassungsrechtlichen Voraussetzungen gehören insbesondere:

a) Es bedarf einer konkreten Gefahr für ein hochrangiges Rechtsgut, wie den Leib, das Leben oder die Freiheit von Bürgerinnen und Bürgern bzw. den Bestand des Bundes oder eines Landes, oder die Maßnahme muss zur Aufklärung besonders schwerer Straftaten erforderlich sein.

b) Die Maßnahme muss zeitlich und örtlich beschränkt angewandt werden. Sie darf nur an sehr eng bestimmten Orten wie etwa Verkehrsknotenpunkten (z. B. Bahnhöfe, Flughäfen) durchgeführt werden, an denen mit dem Auffinden der gesuchten Personen zu rechnen ist, und darf nur so lange andauern, wie die Gefahrenlage besteht oder es für die Aufklärung der Straftaten erforderlich ist.

c) Sie muss von sehr engen technischen und organisatorischen Schutzvorkehrungen flankiert sein. Es bedarf eines Richtervorbehaltes für die Anordnung der Maßnahme und der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit ist zu beteiligen. Die personenbezogenen Daten dürfen nur für die in der Rechtsgrundlage genannten Zwecke verwendet werden und müssen gelöscht werden, wenn der Zweck erreicht ist. Daneben ist ein hohes Maß an Datensicherheit erforderlich.

d) Der Anlass, der Zweck und die Grenzen der Maßnahme müssen in der Ermächtigungsgrundlage bereichsspezifisch, präzise und normenklar festgelegt werden.

Der Gesetzgeber sollte biometrische Gesichtserkennung im öffentlichen Raum nur erlauben, wenn diese gesellschaftlich akzeptiert ist.

Die Frage der gesellschaftlichen Akzeptanz scheint noch nicht geklärt zu sein. Deshalb bedarf es einer breiten öffentlichen demokratischen Debatte.

Wenn die Regulierungsvorschläge der EU-Kommission Gesetz würden, was derzeit noch offen ist, könnte der deutsche Gesetzgeber innerhalb des vorgegebenen Rahmens eine Rechtsgrundlage für die Technologie schaffen. Er sollte aber davon absehen, bis eine breite öffentliche demokratische Debatte abgeschlossen ist („Moratorium“).

6. Über derartig Wesentliches wie den Einsatz von Gesichtserkennungstechnologie zur Strafverfolgung im Nachgang zu Massenereignissen, etwa dem G20-Gipfel, muss der Gesetzgeber entscheiden. Derzeitige Generalklauseln dürften der Rechtsprechung des Bundesverfassungsgerichts hinsichtlich Normenklarheit und Bestimmtheit nicht entsprechen, um den Einsatz der Systeme zu erlauben. Der Gesetzgeber könnte deshalb gefordert sein, eine Spezialrechtsgrundlage für den Einsatz der Technik bei Massenereignissen in der Strafprozessordnung zu schaffen, oder die Exekutive sollte auf deren Einsatz verzichten.

7. Gegen den Einsatz von Gesichtserkennungssystemen zum Abgleich von auf Video aufgenommenen Tatverdächtigen mit polizeilichen Datenbanken bestehen keine grundsätzlichen datenschutzrechtlichen Bedenken.

# 6. Literaturverzeichnis


Beuth, P. (2021). Gesichtserkennung – Hamburgs Datenschützer will Clearview zur Datenlöschung zwingen. In: Der Spiegel (online), 28.01.2021. ↗ https://www.spiegel.de/netzwelt/web/gesichtserkennung-hamburger-datenschuetzer-will-clearview-zur-datenloeschung-zwingen-a-9227eca6-0730-400a-946b-c126d3866353 [19.07.2021].

Bundesverfassungsgericht NJW 1984, 419 – Volkszählungsurteil.

Bundesverfassungsgericht NJW 2006, 1939 – Rasterfahndung.

Bundesverfassungsgericht NVwZ 2007, 688 – Videoüberwachung an öffentlichen Plätzen.

Bundesverfassungsgericht NJW 2008, 822 – Online-Durchsuchung.

Bundesverfassungsgericht MMR 2008, 308 – Kennzeichen I.

Bundesverfassungsgericht NJW 2019, 827 – Kennzeichen II.

Council of Europe, Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (2021a). Guidelines on Facial Recognition. ↗ https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3 [19.07.2021].

Council of Europe, Media Assistance Unit (2021b). Media Release: Facial Recognition: Strict Regulation Is Needed to Prevent Human Rights. ↗ https://search.coe.int/directorate_of_communications/Pages/result_details.aspx?ObjectId=0900001680a12f84 [19.07.2021].

Crumpler, W. (2020). How Accurate are Facial Recognition Systems – and Why Does It Matter? In: CSIS-Blog. ↗ https://www.csis.org/blogs/technology-policy-blog/how-accurate-are-facial-recognition-systems-%E2%80%93-and-why-does-it-matter [19.07.2021].

Dachwitz, I./Laufer, D./Meineck. S. (2020). NPP 204: PimEyes – Gesichtserkennung ist eine Waffe. In: Netzpolitik.org, 18.07.2020. ↗ https://netzpolitik.org/2020/npp-204-pimeyes-gesichtserkennung-ist-eine-waffe/ [19.07.2021].

EU-Kommission (2021a). Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union. Brüssel. ↗ https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0019.02/DOC_1&format=PDF [19.07.2021].

EU-Kommission (2021b). Anhänge des Vorschlags für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz (Gesetz über Künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union. Brüssel. ↗ https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0019.02/DOC_2&format=PDF [19.07.2021].

EU-Kommission (2020). Weißbuch zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen. Brüssel. ↗ https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_de.pdf [19.07.2021].

EUR-Lex (2021). Verfahren 2021/0106/COD. ↗ https://eur-lex.europa.eu/legal-content/DE/HIS/?uri=CELEX%3A52021PC0206 [30.11.2021].

Europäisches Parlament (2021). Entschließung vom 6. Oktober 2021 (2020/2016[INI]). ↗ https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_DE.pdf [30.11.2021].

European Data Protection Board, European Data Protection Supervisor (2021). Joint Opinion 5/2021 on the Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act). ↗ https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en [19.07.2021].

Fanta, A. (2020). Künstliche Intelligenz – EU erwägt Verbot von Gesichtserkennung. In: Netzpolitik.org, 17.01.2020. ↗ https://netzpolitik.org/2020/eu-erwaegt-verbot-von-gesichtserkennung/ [19.07.2021].

Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit (2020). Tätigkeitsbericht. Hamburg. ↗ https://datenschutz-hamburg.de/assets/pdf/29._taetigkeitsbericht_datenschutz_2020.PDF [19.07.2021].

Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit (2019). Datenschutzrechtliche Prüfung des Einsatzes einer Gesichtserkennungssoftware zur Aufklärung von Straftaten im Zusammenhang mit dem G20-Gipfel durch die Polizei Hamburg. ↗ https://datenschutz-hamburg.de/assets/pdf/Pruefbericht_Gesichtserkennungssoftware.pdf [19.07.2021].

Kurz, C. (2021). PimEyes schweigt nach der Flucht auf die Seychellen. In: Netzpolitik.org, 12.07.2021. ↗ https://netzpolitik.org/2021/gesichtserkennung-pimeyes-schweigt-nach-der-flucht-auf-die-seychellen/ [19.07.2021].

Laufer, D. (2020). Gesichtserkennung – Clearview AI verweigert Zusammenarbeit mit deutscher Datenschutzaufsicht. In: Netzpolitik.org, 20.08.2020. ↗ https://netzpolitik.org/2020/gesichtserkennung-clearview-ai-verweigert-zusammenarbeit-mit-deutscher-datenschutzaufsicht/ [19.07.2021].

McLaughlin, M./Castro, D. (2020). The Critics Were Wrong: NIST Data Shows the Best Facial Recognition Algorithms Are Neither Racist Nor Sexist. In: Information Technology and Innovation Foundation, 27.01.2020. ↗ https://itif.org/publications/2020/01/27/critics-were-wrong-nist-data-shows-best-facial-recognition-algorithms [19.07.2021].

Ngan, M. et al. (2020). NIST: Ongoing Face Recognition Vendor Test (FRVT) Part 6A: Face Recognition Accuracy with Masks Using Pre-COVID-19 Algorithms. ↗ https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8311.pdf [19.07.2021].

SPD/Die Grünen/FDP (2021). Koalitionsvertrag 2021 – 2025. ↗ https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag/Koalitionsvertrag_2021-2025.pdf [30.11.2021].

Spiegel-Meldung (2020). Bundespolizeigesetz – Seehofer verzichtet auf Software zur Gesichtserkennung. In: Der Spiegel (online), 24.01.2020. ↗ https://www.spiegel.de/politik/deutschland/bundespolizeigesetz-seehofer-verzichtet-auf-software-zur-gesichtserkennung-a-c207b3c8-eb1a-48e9-80ce-2642b420bd55 [19.07.2021].

Steinacker, L. et al. (2020). Facial Recognition: A Cross-national Survey on Public Acceptance, Privacy and Discrimination. In: ICML 2020 – Law and Machine Learning Workshop. Wien. ↗ https://arxiv.org/abs/2008.07275 [19.07.2021].

Verwaltungsgericht Hamburg, Urteil vom 23.10.2019 – BeckRS 2019, 40195, beck-online.

**bidt – Bayerisches Forschungsinstitut für Digitale Transformation**
Gabelsbergerstraße 4 | 80333 München