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

ANALYSEN UND STUDIEN

Gesichtserkennung

Ein Diskussionsbeitrag zur Regulierung der Technologie

AutorInnen

Nikolaus Bauer, bidt
Jan Gogoll, bidt
Niina Zuber, bidt

Herausgeber

bidt — Bayerisches Forschungsinstitut für Digitale Transformation
www.bidt.digital

Impressum

bidt Analysen und Studien Nr. 6

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

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

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

Layout
Joseph & Sebastian Grafikdesign | www.josephundsebastian.com

Veröffentlichung: November 2021
ISSN: 2701-2379
DOI: 10.35067/xypq-kn64

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 bzw. einer Regulierung der Technologie. Die vorliegende Studie 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 study aims to make a contribution to this debate by considering whether new regulations or a ban are justified.

Inhalt

1 Das Wichtigste in Kürze

a) Die technische Zuverlässigkeit von Gesichtserkennungssystemen nimmt zu. Doch selbst wenn die Technik zu 100 Prozent 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.

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

c) Klassifizierungen mittels Gesichtserkennungssystemen sind auf EU-Ebene 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. Die Europäischen Datenschutzaufsichtsbehörden sollten 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 Gesichtserkennungssysteme 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 drohen können.

d) 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.

e) 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. Sie will sie zudem als hohes Risiko einstufen und strikte obligatorische Auflagen und Verfahren implementieren.

Innerhalb dieses 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:

(1) 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.

(2) 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.

(3) 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.

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

f) 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. Bis zu deren Abschluss sollte der Gesetzgeber davon absehen, eine nationale Rechtsgrundlage für die biometrische Gesichtserkennung im öffentlichen Raum zu schaffen („Moratorium").

g) 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.

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

2 Einleitung

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

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

Auch werden die Systeme technisch immer zuverlässiger. Aber bedeutet technische Zuverlässigkeit gleich, dass die Systeme auch eingesetzt werden dürfen?

Und wie mit den Chancen und Risiken der Technologie richtig umgehen? Bedarf es also 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 jedenfalls ein Moratorium hinsichtlich der biometrischen Gesichtserkennung im öffentlichen Raum geben? Immerhin hat die EU-Kommission bereits über ein solches Moratorium nachgedacht.

Diese Studie versucht, Antworten auf diese Fragen zu geben und einen Beitrag zur aktuellen Diskussion um die Regulierung von Gesichtserkennung zu leisten.

Hierzu wird zunächst eine Einführung in die Technik gegeben, wobei unterschiedliche Arten von Gesichtserkennung voneinander abgegrenzt werden. Hierauf wird die technische Zuverlässigkeit der Systeme besprochen, der bestehende rechtliche Rahmen vorgestellt und möglicher Regulierungsbedarf diskutiert. Abschließend werden eine Zusammenfassung und ein Ausblick gegeben.

3 Einführung

3.1 Was ist Gesichtserkennung?

Definition

„Gesichtserkennung ist die automatische Verarbeitung digitaler Bilder, die Gesichter von natürlichen Personen enthalten, um bei diesen eine Identifizierung, Authentifizierung/Verifizierung oder Kategorisierung [/Klassifizierung] durchzuführen".[1]

Eine normative Bewertung von Gesichtserkennungssystemen bedarf zunächst einer Klärung, welche Art von Technik bzw. Technologie zugrunde gelegt wird. Im ersten Schritt sollen deshalb die Typen der Gesichtserkennungssysteme systematisiert und wesentliche Begriffe geklärt werden.

Gesichtserkennungssysteme haben zum Ziel, eine Person zu authentifizieren, zu identifizieren oder zu klassifizieren.

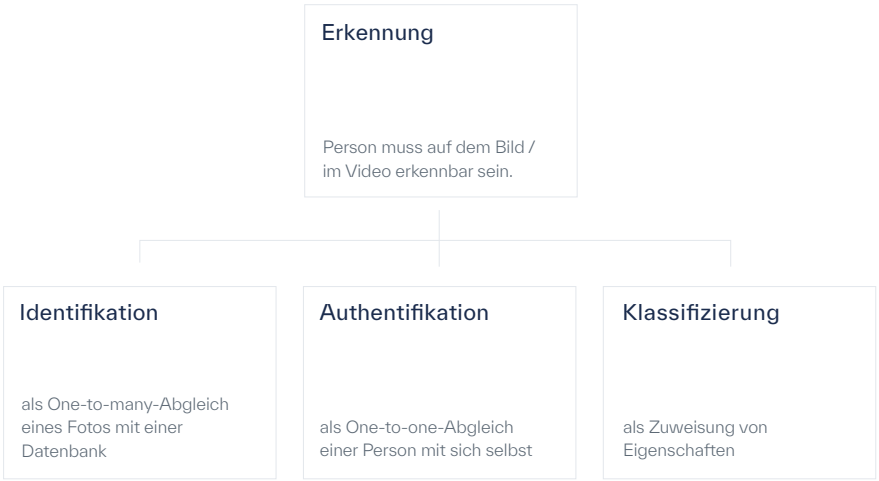

Abbildung 1. Typologie von Gesichtserkennungssystemen

Gesichtserkennung basiert technologisch auf Systemen der Künstlichen Intelligenz (KI). In diesem Teilbereich der Informatik werden Softwaresysteme entwickelt, die unzureichend strukturierte Prozesse automatisieren, also mathematisch abbilden können. Um dieses Problem zu lösen, werden beim Maschinellen Lernen große Mengen an sogenannten Trainings-

1 Artikel-29-Datenschutzgruppe, Stellungnahme 02/2012 zur Gesichtserkennung bei Online- und Mobilfunkdiensten, 2012, S. 2, ↗ https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp192_de.pdf [19.07.2021].

daten benötigt. Die KI-Systeme analysieren diese und versuchen darin Muster und Korrelationen zu erkennen. Wenn die Trainingsdaten gut gewählt sind, lassen sich die damit trainierten Algorithmen dazu verwenden, die gleichen Muster auch in neuen, ihnen unbekannten Daten zu erkennen.

Ethische Probleme der KI

KI-basierte Systeme rufen ethische Probleme hervor, die aus der Opazität oder der Transparenz des informationstechnischen Systems resultieren. Opazität wird in diesem Zusammenhang als „Black Box"-Problematik thematisiert, die aus der Technologie selbst resultiert, wie z. B. bei Neuronalen Netzen. Dies bedeutet, dass konkrete Klassifikationen und Prognosen des Algorithmus selbst von den Entwicklern nicht vollends nachvollziehbar und somit erklärbar sind. Gesichtserkennungssysteme sind transparent, insofern Betroffene das System nicht unmittelbar wahrnehmen können, d. h. Kameras sind nicht ersichtlich, die Klassifikation nicht unmittelbar erkennbar, die Datenspeicherung oder der Betreiber nicht erkennbar etc. Zudem tauchen Diskriminierungs- und Fairnessfragen auf, wenn Algorithmen aufgrund der Limitierung und mangelnder Diversifikation der Trainingsdaten nicht erstrebenswerte reale Phänomene hervorrufen.[2]

3.2 Detektion: Ist auf dem Bild oder Video ein Gesicht zu sehen?

Allen Gesichtserkennungssystemen liegt technisch als erster Schritt das Erkennen von Gesichtern zugrunde. Das bedeutet: Eine Software muss auf einem Foto oder Video einen Bereich als Gesicht klassifizieren. Dies wird als Erkennung bzw. 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 mit Hilfe einer Bewertung von Ähnlichkeiten (engl. similarity score) darstellt".[3]

Es gibt zwei unterschiedliche Anwendungsfälle: die Authentifikation und die Identifikation. Die Klassifikation einer Person stellt technologisch einen anderen Fall der Gesichtserkennung dar.

---

2 Vgl. zu alldem z. B. Floridi u. a., Minds and Machines 2018 (28), S. 689 (692); Arnold/Scheutz, Ethics and Information Technology 2018 (20), S. 59 (60); Morley u. a., Science and Engineering Ethics 2020 (26), S. 214 ff., ↗ https://link.springer.com/content/pdf/10.1007/s11948-019-00165-5.pdf [19.07.2021].

3 Vgl. McLaughlin/Castro, The Critics Were Wrong: NIST Data Shows the Best Facial Recognition Algorithms Are Neither Racist Nor Sexist, ITIF 2020, ↗ https://itif.org/publications/2020/01/27/critics-were-wrong-nist-data-shows-best-facial-recognition-algorithms [19.07.2021].

3.3 Authentifikation: Ist das die Person, für die sie sich ausgibt?

Definition

„Die Verifikation [/Authentifikation] einer Person durch ein biometrisches System erfolgt gewöhnlich durch den Abgleich der (während der Verifikation[/Authentifikation] erfassten) biometrischen Daten einer Person mit einer Reihe biometrischer Templates in einer Datenbank (1-zu-1-Matching)“.[4]

Eine Passkontrolle oder das Entsperren eines Mobiltelefons sind Beispiele für die Authentifikation im Rahmen der Gesichtserkennung, bei der biometrische Daten (z. B. Augenabstand, Stirnbreite) mit einem hinterlegten Datensatz abgeglichen werden. Diese Bestätigung wird deshalb auch als 1-zu-1-Matching bezeichnet.

Frage	Ist das die Person, für die sie sich ausgibt?
Anwendungsbeispiel	Passkontrolle, Entsperren des Telefons
Potenzieller Vorteil	Kostensenkung durch leichtere und schnellere Handhabung des Identitätsnachweises, gezielte und effiziente Sicherung von Grenzen, Zugangskontrollen zu bestimmten Arealen usw.
Potenzieller Nachteil	Erhöhte Schwierigkeit, etwa eine Passkontrolle zu passieren usw.

Fallbeispiel Apple Face ID: Entsperren des Smartphones

Apple Face ID[5] ist eine Authentifikationstechnologie für iPhones, mit der via Gesichtserkennung das Gerät entsperrt oder Zahlungen in Auftrag gegeben werden können. Auf Mobiltelefonen auf Basis des Android-Betriebssystems gibt es vergleichbare Anwendungen.

Die Face-ID-Daten – inklusive der mathematischen Repräsentation des Gesichts, das bei jedem Einloggen getestet wird – werden verschlüsselt auf dem Gerät gespeichert. Laut Aussage von Apple beträgt die Wahrscheinlichkeit, dass eine falsche Person das Smartphone

4 Artikel-29-Datenschutzgruppe, Stellungnahme 3/2012 zu Entwicklungen im Bereich biometrischer Technologien, 2012, S. 6, ↗ https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_de.pdf [19.07.2021], wobei die deutsche Übersetzung fehlerhaft von One-to-many-Verfahren anstatt von One-to-one-Matching spricht, s. die englische (↗ https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf [19.07.2021], S. 6, französische (↗ https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_fr.pdf [19.07.2021], S. 6, und spanische Sprachversion (↗ https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_es.pdf [19.07.2021], S. 6.

5 Vgl. Apple, About Face ID Advanced Technology, 2020, ↗ https://support.apple.com/en-gb/HT208108 [19.07.2021].

entsperren kann, eins zu einer Million. Mit geschlossenen Augen funktioniert die Erkennung nicht, möglich ist sie mit Brillen, Hüten und Bärten. Anpassungen an sich verändernde Erscheinungsweisen (im Vergleich zum Ausgangsbild) werden durch Machine-Learning-Algorithmen aufgefangen. Schwierigkeiten treten bei Zwillingen oder ähnlich aussehenden Geschwistern auf.[6]

Kritik an Apple Face ID ist weniger technologisch ausgerichtet, sondern thematisiert z. B. das Problem, dass Dritte das Gerät entsperren können, indem sie es (etwa gewaltsam) vor das Gesicht der Besitzerin oder des Besitzers halten.

3.4 Identifikation: Wer ist die Person auf dem Bild?

Definition

„Die Identifikation einer Person durch ein biometrisches System erfolgt gewöhnlich durch den Abgleich biometrischer Daten einer Person (die während der Identifikation erfasst wurden) mit einer Reihe biometrischer Templates in einer Datenbank (One-to-many-Verfahren)“.[7]

Das Szenario einer polizeilichen Fahndung entspricht der Identifikation durch ein Gesichtserkennungssystem: Ein Gesicht aus einem Foto oder Video soll in einer Menge von Einträgen in vorhandenen Datenbanken gefunden (oder zumindest eine Liste von potenziell infrage kommenden Personen erstellt) werden. Diese Art der Gesichtserkennung entspricht einem One-to-many-Matching. Rechtlich ist die anlassbezogene und anlasslose Überprüfung zu unterscheiden. Dies bestimmt auch die politische Diskussion.

Frage	Wer ist die Person auf dem Bild?
Anwendungsbeispiel	Polizei gleicht Videoausschnitt im Rahmen von Ermittlungsarbeit mit einer Datenbank ab
Potenzieller Vorteil	Kostensenkung der Strafverfolgung und höhere Effizienz der Verfolgung
Potenzieller Nachteil	Fehlerquote, z. B. unschuldige Person gerät in den Fokus der Ermittlungsbehörden usw., fehlerhafte Zuordnung von Bildmaterial

6 Vgl. Apple (Fn. 5).

7 Artikel-29-Datenschutzgruppe (Fn. 4), S. 6.

Fallbeispiel: Automatisierte Gesichtserkennung am Bahnhof Berlin Südkreuz

Von Juli bis August 2017 fand in Deutschland der erste groß angelegte Test von automatisierter Gesichtserkennung in Echtzeit am Bahnhof Berlin Südkreuz statt. „Der Einsatz von Videotechnik im öffentlichen Raum leistet wertvolle Unterstützung bei der polizeilichen Kriminalitätsbekämpfung", begründete die Bundespolizei ihren Einsatz.[8]

Drei Kameras filmten über zwei mehrmonatige Testphasen hinweg mit drei unterschiedlichen Softwaresystemen zwei Ausgänge und eine Rolltreppe, um etwa 300 freiwillige Zielpersonen zu identifizieren. Das beste Softwaresystem lieferte in der zweiten Testphase eine für alle drei Kameras durchschnittliche Trefferquote von 82,8 %, in Kombination aller drei Systeme kam man auf mehr als 90 %. Die Falschakzeptanzrate (falsch positiv) konnte in diesem Kombimodus unter 0,1 % gedrückt werden.[9]

Der Test eröffnete die erste große Welle an politischer Diskussion zu Gesichtserkennungssystemen in Deutschland. Die Datenschutzbeauftragten, Oppositionsparteien sowie zivilgesellschaftliche Interessengruppen kritisierten den Test. Der Chaos Computer Club warf der Bundespolizei etwa vor, die Ergebnisse durch die Kombination dreier Softwaresysteme schönzurechnen.[10] Bundespolizei und Bundesinnenministerium werteten den Test als Erfolg.

3.5 Klassifizierung: Wie soll eine bestimmte Person klassifiziert werden?

Definition

„Die Kategorisierung [/Klassifizierung] der Merkmale einer Person durch ein biometrisches System erfolgt gewöhnlich, indem festgestellt wird, ob die biometrischen Daten einer Person einer Gruppe mit vordefinierten Merkmalen zuzuordnen sind, um dann bestimmte Maßnahmen einzuleiten. In diesem Fall kommt es nicht darauf an, die betreffende Person zu identifizieren oder zu verifizieren [/authentifizieren], sondern die Person automatisch einer bestimmten Kategorie zuzuweisen".[11]

Technologien zur Gesichtserkennung lassen sich auch dazu einsetzen, eine Person bestimmten Kategorien zuzuordnen: Wie alt ist sie? Welches Geschlecht, welcher Hautton, welche Emotion ist sichtbar?

---

8 Bundespolizeipräsidium, Abschlussbericht „Biometrische Gesichtserkennung" des Bundespolizeipräsidiums im Rahmen der Erprobung von Systemen zur intelligenten Videoanalyse durch das Bundesministerium des Innern, für Bau und Heimat, das Bundespolizeipräsidium, das Bundeskriminalamt und die Deutsche Bahn AG am Bahnhof Berlin Südkreuz, 2018, S. 35, ↗ https://www.bundespolizei.de/Web/DE/04Aktuelles/01Meldungen/2018/10/181011_abschlussbericht_gesichtserkennung_down.pdf [19.07.2021].

9 Vgl. Bundespolizeipräsidium (Fn. 8), S. 25.

10 Vgl. Chaos Computer Club, Biometrische Videoüberwachung: Der Südkreuz-Versuch war kein Erfolg, 2018, ↗ https://www.ccc.de/de/updates/2018/debakel-am-suedkreuz [19.07.2021].

11 Artikel-29-Datenschutzgruppe (Fn. 4), S. 6.

Um Fragen dieser Art zu beantworten, bedarf es technisch weder einer Identifikation noch einer Authentifikation, sondern das Softwaresystem kategorisiert nach definierten Kriterien. Einem bestimmten Alter werden etwa sogenannte „Faltigkeitsintervalle", bestimmten Farbtönen verschiedene Hautfarben und einer bestimmten Haltung der Mundwinkel die emotionale Verfasstheit einer Person (sogenannte Sentiment Analysis) zugeordnet. Diese Kriterien können so zustande kommen: (1) Ein Mensch definiert manuell eine Skala. (2) Methoden des Maschinellen Lernens leiten die Kriterien aus den Trainingsdaten ab. (3) Es wird eine Kombination aus (1) und (2) vorgenommen.

Frage	Wie soll eine bestimmte Person klassifiziert werden (z. B. hinsichtlich Alter, Aufmerksamkeitsgrad, Stimmung)?
Anwendungsbeispiel	Unfallverhütung bei Sekundenschlaf, verbesserte Diagnose von Krankheiten
Potenzielle Vorteile	Feststellung der Müdigkeit des Fahrers eines Kraftfahrzeugs (driver drowsiness detection), verbesserte Diagnose von Krankheiten usw.
Potenzielle Nachteile	Assistenzsystem reagiert falsch, Fehldiagnosen, Diskriminierungspotenzial usw.

Fallbeispiel: Gesichtserkennung in der Medizin

Ein Einsatz im medizinischen Bereich ist darauf ausgelegt, Krankheitsbilder oder Gesundheitszustände zu erkennen.[12] Eine Klassifizierung erlaubt Gesundheitszustände einzugruppieren, um beispielsweise genetische Krankheitsbilder, die sich vor allem in einer bestimmten Gesichtsphysiognomie zeigen, zu erkennen.[13] So weist der Algorithmus DeepGestalt, der hinter der Applikation Face2Gene liegt, bei der Zuordnung des Noonan-Syndroms eine höhere Trefferquote als Ärztinnen und Ärzte auf. Allerdings muss man hinzufügen, dass in einem lebensweltlichen Diagnosekontext Ärztinnen und Ärzte viele Krankheitsbilder miteinander vergleichen können müssen, was dieser Applikation (noch) nicht gelingt. Ergänzt man solche Anwendungen um eine Analyse von Sprache oder Emotionen, könnte es möglich sein, psychische Erkrankungen, wie Depressionen, zuverlässig zu kategorisieren.[14]

12 Vgl. Martinez-Martin, AMA Journal of Ethics 2019 (21, 2), S. 180 ff., ↗ https://journalofethics.ama-assn.org/sites/journalofethics.ama-assn.org/files/2019-01/pfor1-1902_0.pdf [19.07.2021].

13 Vgl. The Medical Futurist, Your Guide to Facial Recognition Technology in Healthcare, 2019, ↗ https://medicalfuturist.com/your-guide-to-facial-recognition-technology-in-healthcare/ [19.07.2021].

14 Vgl. Gurovich u. a. Nature Medicine 2019 (25), S. 60 ff.

Stellungnahme

Der Einsatz digitaler Systeme kann die medizinische Diagnostik unterstützen. Falsche Klassifikationen können jedoch zu Benachteiligungen oder Fehlentscheidungen führen, wie etwa Fehldiagnosen oder Fehlmedikation aufgrund äußerer Merkmale.

Die verschieden Typen von Gesichtserkennung und ihre potenziellen Vor- und Nachteile zusammengefasst

	Detektion	Authentifizierung	Identifikation	Klassifizierung
Anwendungs-beispiele	Grundlage für alle weiteren Gesichts-erkennungstechnologien	Passkontrolle, Entsperren des Telefons	Polizei gleicht Video-ausschnitt im Rahmen von Ermittlungsarbeit mit Datenbank ab	Altersfeststellung, Aufmerksamkeitskontrolle
Antwort auf	Ist auf dem Bild oder Video ein Gesicht zu sehen?	Ist das die Person, für die sie sich ausgibt?	Wer ist die Person auf dem Bild?	Wie soll eine bestimmte Person klassifiziert werden?
Potenzielle Vorteile	Gesichter erkennen und zuordnen	Kostensenkung, besserer und einfacherer Identitäts-nachweis	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 unzu-treffenderweise Persönlich-keitsmerkmale zugeordnet

4 Technische Zuverlässigkeit

KI-Systeme sind lernende, probabilistische Systeme. Probabilistisch bedeutet, dass das Ergebnis der Gesichtserkennungs-KI immer als Wahrscheinlichkeit ausgegeben wird, wobei das Ziel ist, so nahe wie möglich an 100 % Wahrscheinlichkeit zu gelangen. Lernend heißt, dass die Systeme lernen, Gesichter zu erkennen und anschließend zu authentifizieren, identifizieren oder zu klassifizieren.[15] Im Gegensatz zu deterministischen Systemen verändern sich sowohl die Ergebnisse als auch das Modell selbst, je nach Inputdaten: „In der Praxis hat dies zur Folge, dass sich die Güte von KI-Systemen nie allgemein und durch das Verfahren selbst, sondern immer nur durch Anwendung auf einen konkreten Satz an Eingabedaten bewerten lässt".[16]

Eine solche Bewertung auf Basis von Benchmark-Datensätzen führt regelmäßig das US-amerikanische National Institute of Standards and Technology (NIST) mit dem Face Recognition Vendor Test (FRVT) durch. Die Untersuchungen des NIST zeigen: Die Zuverlässigkeit von Gesichtserkennungssystemen hat in den vergangenen Jahren zugenommen. Unter idealen Bedingungen liegt die Zuverlässigkeit bestimmter Systeme bei bis zu 99,97 %.[17]

Stellungnahme

Eine Fehlerquote von 0,03 % bedeutet, dass unter 10.000 Personen drei Personen falsch erkannt werden. Eine falsche Behandlung hat Diskriminierungspotenzial für die betroffenen Personen.

Eine Hauptursache für Fehler in solchen Systemen sind die zugrunde liegenden Trainingsdatensätze: Je weniger divers oder repräsentativ ein Datensatz für den gewünschten Output ist, desto höher die Wahrscheinlichkeit, dass eine Gruppe unterrepräsentiert und somit für den Algorithmus nicht oder nur schwer klassifizierbar ist.[18] Neben den Trainingsdaten, der Grundlage für das Modell eines Algorithmus, müssen auch die Benchmark-Datensätze, mit denen Systeme auf ihre technische Zuverlässigkeit hin geprüft werden, repräsentative und diverse Bilder enthalten. Dies ist insbesondere für Minderheiten wichtig.

---

15 Vgl. Council of Europe, Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Azria/Wickert), Facial Recognition: Current Situation and Challenges, 2019, S. 3, ↗ https://rm.coe.int/t-pd-2019-05rev-facial-recognition-report-003-/16809eadf1 [19.07.2021].

16 Vgl. Beining, Vertrauenswürdige KI durch Standards? Herausforderungen bei der Standardisierung und Zertifizierung von Künstlicher Intelligenz, Stiftung Neue Verantwortung 2020, S. 13, ↗ https://www.stiftung-nv.de/sites/default/files/herausforderungen-standardisierung-ki.pdf [19.07.2021].

17 Vgl. Crumpler, How Accurate Are Facial Recognition Systems – and Why Does It Matter?, in: CSIS-Blog, 2020, ↗ 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].

18 Vgl. dazu Choudhury, 10 Face Datasets to Start Facial Recognition Projects, in: Analytics India Magazine, 2020, ↗ https://analyticsindiamag.com/10-face-datasets-to-start-facial-recognition-projects/ [19.07.2021]: Datensätze können erworben werden und rangieren vom Datenset Real and Fake Face Detection über Labelled Faces in the Wild Home (LFW) bis hin zum Dataset-large-scale CelebFaces Attributes (CelebA) Dataset 2015. Der Tufts-Face-Datensatz beispielsweise umfasst zudem Fotos von Nahaufnahmen, Fernaufnahmen, bearbeiteten und 3-D-Daten.

Trotz der positiven Evaluierung stehen Gesichtserkennungssysteme in Verdacht, bei Frauen und Menschen mit dunkleren Hauttypen schlechter zu funktionieren. Wegweisend war dafür 2018 die Studie *Gender Shades*.[19] Die Studie zeigt, dass zwei gängige Benchmark-Datensätze, mit denen Algorithmen evaluiert werden (u. a. IJB-A von NIST), zu einem überwiegenden Teil aus hellhäutigen Gesichtern bestehen. Mit einem neuen Datensatz, der helle und dunklere Hauttöne für Männer und Frauen ausgeglichen enthält, testeten IBM, Microsoft und Megvii drei kommerzielle Klassifizierungsalgorithmen: Die Algorithmen lieferten zuverlässigere Ergebnisse bei Männern und hellhäutigen Gesichtern, jedoch nicht bei Frauen und dunkleren Hauttypen. In einer Nachfolgestudie aus dem Jahr 2020 mit einem anderen Benchmark-Datensatz und einem Audit der Algorithmen von Microsoft, Amazon und Clarifai zeigten die beiden erstgenannten so gut wie keine Unterschiede mehr beim Erkennen des Geschlechts bei verschiedenen Hauttypen. Die Autorinnen und Autoren der Studie sehen das als Indiz dafür an, dass öffentliche Kritik Wirkung gezeigt hat. Performance-Unterschiede gibt es allerdings weiterhin bei der Bestimmung des Alters.[20]

Die Bildqualität ist ein weiterer Faktor, der sich auf die technische Zuverlässigkeit auswirkt. Man kann davon ausgehen, dass unter kontrollierten Rahmenbedingungen, beispielsweise bei einer Passkontrolle am Flughafen mit stabilen Lichtverhältnissen und einem Abgleich mit biometrischen Fotos, die Zuverlässigkeit auch außerhalb von Testszenarien sehr hoch bleibt. Verschwommene oder verpixelte Bilder und Videomaterial ohne Frontalansicht erschweren die Authentifikation und Identifikation jedoch erheblich. Ein Test von NIST zeigt etwa, dass Mund-Nase-Bedeckungen während der Coronapandemie zu hohen Fehlerquoten führen.[21] Das zeigt: Sich verändernde Bedingungen wirken sich auf die Zuverlässigkeit von Gesichtserkennungssystemen aus.

Fazit

Die technische Zuverlässigkeit von Gesichtserkennungssystemen hängt stark von der Qualität der Trainingsdaten ab. Je weniger divers oder je weniger repräsentativ ein Datensatz ist, desto höher die Wahrscheinlichkeit, dass eine Gruppe unterrepräsentiert ist und somit für den Algorithmus nicht oder nur schwer klassifizierbar ist. Die technische Zuverlässigkeit von Gesichtserkennungssystemen nimmt zu. Dennoch bleibt auch unter idealen Bedingungen eine Fehlerquote. Selbst wenn diese nur bei 0,03 % liegt, bedeutet das, dass unter 10.000 Personen drei Personen falsch erkannt werden. Eine falsche Behandlung hat Diskriminierungspotenzial für die betroffenen Personen.

---

19 Vgl. Buolamwini/Gebru, PMLR 2018 (81), S. 1 ff., ↗ http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf [19.07.2021].

20 Vgl. Raji, AIES 2020: Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society 2020, S. 145 (146).

21 Vgl. Ngan/Grother/Hanaoka, Ongoing Face Recognition Vendor Test (FRVT) Part 6a: Face Recognition Accuracy with Masks Using Pre-COVID-19 Algorithms, NIST, 2020, S. 5 (ii), ↗ https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8311.pdf [19.07.2021].

5 Rechtlicher Rahmen

Wenn Systeme technisch nicht zuverlässig sind, können sie nicht ohne Weiteres durch öffentliche Stellen gegenüber Bürgerinnen und Bürgern eingesetzt werden, denn der verfassungsrechtliche Grundsatz der Verhältnismäßigkeit[22] 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?[23] Technische Unzuverlässigkeit kann ebenfalls bedeuten, dass die Systeme ungleich behandeln, beispielsweise Menschen mit helleren und dunkleren Hauttypen oder Männer und Frauen, und so gegen den Gleichheitssatz des Grundgesetzes[24] verstoßen.

Auch zwischen Privaten müssen Gesichtserkennungssysteme 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 Gesichtserkennungssysteme einsetzt, muss weitere verfassungsrechtliche und datenschutzrechtliche Anforderungen beachten.

5.1 Verfassungsrechtliche Anforderungen

Verfassungsrechtlich stellt biometrische Gesichtserkennung durch öffentliche Stellen einen Eingriff in das Recht auf informationelle Selbstbestimmung der betroffenen Bürgerinnen und Bürger dar. Vor dem Hintergrund moderner Datenverarbeitung, die eine immer umfassendere Datenverarbeitung und Datenvernetzung erlaubt und die Gefahr einer „totalen Registrierung und Katalogisierung“ birgt,[25] hat das Bundesverfassungsgericht im sogenannten Volkszählungsurteil im Jahr 1983 das Recht auf informationelle Selbstbestimmung als Ausprägung des allgemeinen Persönlichkeitsrechts[26] entwickelt. Das Freiheitsrecht gewährleistet die Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden, und schützt die Bürgerinnen und Bürger vor einer unbegrenzten Erhebung, Speicherung, Verwendung und Weitergabe ihrer persönlichen Daten.[27]

---

22 Nach dem verfassungsrechtlichen Grundsatz der Verhältnismäßigkeit muss eine Maßnahme einen legitimen Zweck verfolgen, geeignet sein, diesen Zweck zu erreichen, sowie erforderlich und angemessen sein.

23 Vgl. European Union Agency for Fundamental Rights, Facial Recognition Technology: Fundamental Rights Consideration in the Context of Law Enforcement, 2019, S. 22, ↗ https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf [19.07.2021].

24 Art. 3 GG.

25 Di Fabio, in: Maunz/Dürig, Grundgesetz, Band 1, 94. Auflage 2021, Art. 2 Abs. 1 GG, Rn. 173.

26 Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG.

27 Grundlegend BVerfG NJW 1984, 419 (422) - Volkszählungsurteil.

Eingriffe dürfen demnach durch den Gesetzgeber nur vorgenommen werden, wenn die Betroffenen zustimmen oder es eine gesetzliche Grundlage für den Eingriff gibt, die verhältnismäßig ist, den Grundsätzen der Normenbestimmtheit und Normenklarheit entspricht und hinreichende organisatorische und verfahrensrechtliche Schutzvorkehrungen aufweist.[28]

Verhältnismäßigkeit

Verhältnismäßig ist der Eingriff, wenn er ein legitimes Ziel verfolgt, geeignet ist, dieses Ziel zu erreichen, nicht weiter geht, als es zum Schutz des Interesses notwendig ist, und verhältnismäßig im engeren Sinne ist. Die Verhältnismäßigkeit im engeren Sinne lässt sich so auf den Punkt bringen: Der Zweck heiligt nicht die Mittel. Vielmehr gilt: Die Schwere eines Eingriffs darf bei einer Gesamtabwägung nicht außer Verhältnis zu dem Gewicht der ihn rechtfertigenden Gründe stehen.[29]

Gebot der Normenbestimmtheit und der Normenklarheit

Das Gebot der Normenbestimmtheit und der Normenklarheit soll sicherstellen, dass der demokratisch legitimierte Gesetzgeber die wesentlichen Entscheidungen selbst trifft und das Handeln der Verwaltung gesteuert und begrenzt wird. Auch sollen Bürgerinnen und Bürger sowie die Gerichte den Inhalt der Norm klar und bestimmt erkennen können, um sich darauf einstellen bzw. eine Rechtskontrolle durchführen zu können.[30] Der Anlass, der Zweck und die Grenzen des Eingriffs müssen in der Ermächtigung bereichsspezifisch, präzise und normenklar festgelegt werden.[31] Je schwerer ein Eingriff wiegt, desto höher sind die Anforderungen an die Klarheit und Bestimmtheit der Rechtsgrundlage.[32] Das Bundesverfassungsgericht hat etwa eine datenschutzrechtliche Generalklausel als zu unbestimmt für eine Videoüberwachung angesehen, da es sich im Hinblick auf die Anlasslosigkeit und große Streubreite der Maßnahme um einen sehr intensiven Grundrechtseingriff handelte.[33]

Organisatorische und verfahrensrechtliche Vorkehrungen

Organisatorische und verfahrensrechtliche Vorkehrungen sind dazu bestimmt, Missbrauchsmöglichkeiten auszuschließen.[34] Hierzu gehört die Pflicht der Verantwortlichen, die Betroffenen über die Datenverarbeitung aufzuklären sowie ihnen Auskunft über gespeicherte Daten zu gewähren. Auch sind zur Zweckerreichung nicht (mehr) erforderliche Daten zu löschen. Die Verwendung der Daten ist grundsätzlich auf den gesetzlich bestimmten Erhebungszweck begrenzt. Zudem sind unabhängige Datenschutzbeauftragte zu beteiligen.[35] Daneben kann ein hohes Maß an Datensicherheit notwendig sein (beispielsweise „eine getrennte Speicherung der Daten, eine anspruchsvolle Verschlüsselung, ein gesichertes Zugriffsregime unter Nutzung etwa des Vier-Augen-Prinzips sowie eine revisionssichere Protokollierung“[36]). Auch kann ein Richtervorbehalt hierzu gehören.[37]

28 Grundlegend BVerfG NJW 1984, 419 (422) - Volkszählungsurteil.

29 Etwa BVerfG MMR 2008, 308 (314) - Kennzeichen I.

30 BVerfG MMR 2008, 308 (310 f.) - Kennzeichen I.

31 BVerfG MMR 2008, 308 (311) - Kennzeichen I.

32 BVerfG MMR 2008, 308 (309) - Kennzeichen I.

33 BVerfG NVwZ 2007, 688 (690 f.) - Videoüberwachung an öffentlichen Plätzen.

34 Grundlegend BVerfG NJW 1984, 419 - Volkszählungsurteil.

35 Grundlegend BVerfG NJW 1984, 419 (422) - Volkszählungsurteil.

36 BVerfG MMR 2010, 356 (361) - Vorratsdatenspeicherung: Zu Art. 10 GG, die Erwägungen lassen sich wohl aber auf schwere Eingriffe in das Recht auf informationelle Selbstbestimmung übertragen.

37 BVerfG NJW 2008, 822 (832) - Online-Durchsuchung.

5.2 Datenschutzrechtliche Anforderungen

Europarechtlich wird die Verarbeitung personenbezogener Daten zum einen durch die Datenschutz-Grundverordnung (EU/VO/2016/679, im Folgenden: DSGVO) und zum anderen durch die Datenschutzrichtlinie im Bereich Justiz und Inneres (EU/RL/2016/680, im Folgenden: JI-Richtlinie) reguliert. Während die JI-Richtlinie die Verarbeitung personenbezogener Daten zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung regelt, betrifft die DSGVO die Datenverarbeitung für sonstige Zwecke. Beim Einsatz von Gesichtserkennungssystemen zur Authentifikation und Identifikation werden besondere Kategorien personenbezogener Daten verarbeitet. Es handelt sich um biometrische Daten, nämlich um „Gesichtsbilder, [...] die die eindeutige Identifikation dieser natürlichen Person ermöglichen oder bestätigen".[38] Erfolgt die 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 besondere Kategorien personenbezogener Daten, etwa Gesundheitsdaten,[39] handeln.[40]

Nach der JI-Richtlinie ist die Verarbeitung besonderer Kategorien personenbezogener Daten nur dann erlaubt, wenn sie unbedingt erforderlich ist, vorbehaltlich geeigneter Garantien für die Rechte und Freiheiten der betroffenen Person erfolgt und wenn sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zulässig ist.[41] Nach der DSGVO ist die Verarbeitung besonderer Kategorien personenbezogener Daten zulässig, wenn die betroffene Person eingewilligt hat[42] oder eine gesetzliche Rechtsgrundlage vorliegt[43]. Dies ist insbesondere die Wahrung eines erheblichen öffentlichen Interesses oder die Gesundheitsvorsorge.

Für die Verarbeitung personenbezogener Daten gelten bestimmte Grundsätze.[44] Diese Grundsätze finden im „gesamten Zyklus der Datenverarbeitung"[45] Anwendung und werden in den Einzelvorschriften der DSGVO, der JI-Richtlinie und des BDSG konkretisiert. Sie stellen eine Ausprägung des Verhältnismäßigkeitsgrundsatzes dar.[46] Gesichtserkennungssysteme haben diese datenschutzrechtlichen Grundsätze bzw. die sie konkretisierenden Normen der DSGVO, der JI-Richtlinie und des BDSG einzuhalten.

---

38 Art. 3 Nr. 13 JI-Richtlinie bzw. Art. 4 Nr. 14 DSGVO.

39 Art. 4 Nr. 15 DSGVO.

40 Vgl. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, Positionspapier zur biometrischen Analyse, 2019, S. 18 ff., ↗ https://www.datenschutzkonferenz-online.de/media/oh/20190405_positionspapier-biometrie.pdf [19.07.2021].

41 Art. 10 lit. a) JI-Richtlinie.

42 Art. 9 Abs. 2 lit. a) DSGVO.

43 Art. 9 Abs. 2 lit. b)-j) DSGVO.

44 Art. 5 DSGVO bzw. Art. 4 JI-Richtlinie (umgesetzt in § 47 BDSG).

45 Heberlein, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Auflage 2018, Art. 5 Rn. 1.

46 Braun, in: Gola/Heckmann, Bundesdatenschutzgesetz, 13. Auflage 2019, § 47 Rn. 2.

Datenschutzrechtliche Grundsätze

Grundsatz der Rechtmäßigkeit, Grundsatz von Treu und Glauben, Grundsatz der Transparenz

Eine Datenverarbeitung ist rechtmäßig, sofern sie auf eine Einwilligung oder eine gesetzliche Rechtsgrundlage gestützt werden kann (Verbot mit Erlaubnisvorbehalt). Die Rechtsgrundlage muss normenklar formuliert sein und den Zweck der Datenverarbeitung erkennen lassen.[47] Der Grundsatz von Treu und Glauben erfordert eine „faire Verarbeitung", insbesondere muss eine Einwilligung freiwillig erteilt worden sein.[48] Der Grundsatz der Transparenz verlangt, dass betroffene Personen in verständlicher und klarer Weise Kenntnis davon erlangen, von wem zu welchem Zweck welche Art von personenbezogenen Daten wie lange verarbeitet werden, welche diesbezüglichen Rechte bestehen und wie diese Rechte geltend gemacht werden können.[49] Da im Anwendungsbereich der JI-Richtlinie zum Zwecke der Strafverfolgung bzw. der Gefahrenabwehr heimliche Ermittlungsmaßnahmen gerade notwendig sind, gilt dort der Grundsatz der Transparenz nicht. Allerdings müssen betroffene Personen nachträglich über Maßnahmen unterrichtet werden, um ihre Rechte wahrnehmen zu können.[50]

Grundsatz der Zweckbindung

Personenbezogene Daten dürfen nur für eindeutige, im Voraus festgelegte und legitime Zwecke erhoben werden. Die Verarbeitung ist grundsätzlich auf diese Zwecke beschränkt, ausnahmsweise dürfen die Daten auch für andere Zwecke weiterverarbeitet werden.[51]

Grundsatz der Datenminimierung

Insbesondere dürfen personenbezogene Daten nur verarbeitet werden, sofern das erforderlich, d. h. notwendig ist. Die Erforderlichkeit ist nicht gegeben, wenn ein milderes, gleich geeignetes Mittel zur Verfügung steht. Auch muss die Intensität der Datenverarbeitung in einem angemessenen Verhältnis zu ihrem Zweck stehen.[52]

Grundsatz der Richtigkeit

Personenbezogene Daten müssen richtig sein. Dies hat der Verantwortliche selbst zu überprüfen.[53]

Grundsatz der Speicherbegrenzung

Personenbezogene Daten dürfen nicht länger gespeichert werden, als dies für die Erreichung der Zwecke der Verarbeitung erforderlich ist.[54]

Integrität und Vertraulichkeit von personenbezogenen Daten

Personenbezogene Daten müssen so verarbeitet werden, dass ihre Sicherheit angemessen gewährleistet ist. Durch technische und organisatorische Maßnahmen ist daher sicherzustellen, dass es nicht zu „unbefugter oder unrechtmäßiger Verarbeitung, zu unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung" kommt.[55]

---

47 Braun (Fn. 46), § 47 Rn. 10.

48 Heberlein (Fn. 45), Art. 5 Rn. 9 f.

49 Heberlein (Fn. 45), Art. 5 Rn. 12.

50 Braun (Fn. 46), § 47 Rn. 14.

51 Braun (Fn. 46), § 47 Rn. 15 ff.

52 Braun (Fn. 46), § 47 Rn. 21 ff.

53 Braun (Fn. 46), § 47 Rn. 26 ff.

54 Braun (Fn. 46), § 47 Rn. 30 f.

55 Braun (Fn. 46), § 47 Rn. 32.

Hat eine Datenverarbeitung, insbesondere bei der Verwendung neuer Technologien, voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, ist überdies eine Datenschutzfolgenabschätzung durchzuführen.

Datenschutzfolgenabschätzung[56]

Bei besonders riskanten Datenverarbeitungsvorgängen ist eine Datenschutzfolgenabschätzung vorzunehmen. Eine Datenschutzfolgenabschätzung hat das Ziel, dass die Vorgaben der DSGVO bzw. der JI-Richtlinie und des BDSG eingehalten werden. Die Risiken für Einzelne sollen eingeschätzt und anschließend durch Maßnahmen minimiert werden.[57] Verbleibt dennoch ein hohes Restrisiko, so ist die Datenschutzaufsichtsbehörde zu konsultieren, gegebenenfalls hat die Datenverarbeitung zu unterbleiben.[58] Bei der Verarbeitung von personenbezogenen Daten durch Gesichtserkennungssysteme dürfte eine Datenschutzfolgenabschätzung durchzuführen sein.[59]

Wenn die Datenverarbeitung durch das Gesichtserkennungssystem zulässig war, gibt es darüber hinaus eine Vorschrift in der Datenschutz-Grundverordnung und im Bundesdatenschutzgesetz, die normiert, ob man auf Basis der Datenverarbeitung durch die Gesichtserkennungssoftware eine Entscheidung treffen darf, z. B. eine bestimmte medizinische Behandlung anhand des Befundes des Gesichtserkennungssystems vornehmen darf oder eine Person verhaften darf, wenn das Gesichtserkennungssystem zu dem Ergebnis kommt, es handele sich um eine gesuchte Person in einer Fahndungsdatenbank. Die Vorschrift regelt also die anschließende „Nutzung bestimmter Ergebnisse einer Datenverarbeitung".[60]

Verbot automatisierter Entscheidungen im Einzelfall[61]

Die Vorschrift soll Bürgerinnen und Bürger davor schützen, dass Entscheidungen ausschließlich auf Basis einer automatisierten Datenverarbeitung getroffen werden und „der Einzelne so zu einem bloßen Objekt computergestützter Programme wird".[62] Ein Mensch muss also stets die automatisierte Datenverarbeitung, z. B. das Ergebnis eines Gesichtserkennungssystems, inhaltlich überprüfen und die Entscheidung treffen. Ein Mensch hat die Entscheidung inhaltlich zu verantworten.[63] Ausschließlich automatisierte Entscheidungen sind grund-

---

56 Art. 35 DSGVO, Art. 27 JI-Richtlinie, umgesetzt in § 67 BDSG.

57 Jandt, in: Kühling/Buchner, Datenschutz-Grundverordnung, 3. Auflage 2020, Art. 35 Rn. 1.

58 Vgl. Art. 36 DSGVO; vgl. auch Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, Kurzpapier Nr. 5, Datenschutzfolgenabschätzung nach Art. 35 DSGVO, 2018, S. 5, ↗ https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf [19.07.2021].

59 Vgl. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist, 2018, ↗ https://www.lda.bayern.de/media/dsfa_muss_liste_dsk_de.pdf [19.07.2021], im Hinblick auf Authentifikation und Identifikation: Nr. 1 „Verarbeitung von biometrischen Daten", im Hinblick auf Klassifizierung: Nr. 11 „Einsatz von Künstlicher Intelligenz zur [...] Bewertung persönlicher Aspekte der betroffenen Person".

60 Buchner (Fn. 57), Art. 22 Rn. 11.

61 Art. 22 DSGVO, Art. 11 JI-Richtlinie, umgesetzt in § 54 BDSG.

62 Buchner (Fn. 57), Art. 22 Rn. 1.

63 Buchner (Fn. 57), Art. 22 Rn. 15.

sätzlich verboten, wenn sie dem Einzelnen gegenüber rechtliche Wirkung entfalten oder ihn in ähnlicher Weise erheblich beeinträchtigen.

Doch es gibt Ausnahmen von dieser Regel. Eine Ausnahme ist, wenn die betroffene Person ausdrücklich darin eingewilligt hat, dass die Maschine die Entscheidung treffen soll.[64]

Doch selbst wenn Betroffene ausdrücklich eingewilligt haben, so müssen Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Personen vorhanden sein. Das bedeutet, die Verarbeitung muss „fair und transparent" sein.[65] Fair, da betroffene Personen stets die Möglichkeit haben müssen, dass doch wieder ein Mensch die Entscheidung inhaltlich verantwortet und dabei auch ihren eigenen Standpunkt berücksichtigt.[66] Betroffene müssen nämlich die Möglichkeit haben, zu erwirken, dass eine Person in die automatisierte Datenverarbeitung eingreift, sie ihren eigenen Standpunkt darlegen können und dass sie die automatisierte Entscheidung anfechten können.[67]

Über diese Rechte müssen betroffene Personen im Vorfeld der Verarbeitung transparent unterrichtet werden, um dann ihre Rechte auch wahrnehmen zu können.[68] Auch müssen sie über das Bestehen der automatisierten Entscheidungsfindung einschließlich Profiling, die involvierte Logik, die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung unterrichtet werden.[69]

Das Verbot automatisierter Entscheidung im Einzelfall betrifft Fälle, dass automatisierte Datenverarbeitungen Bewertungen vornehmen, also beispielsweise Gesichtserkennungssysteme zu dem Ergebnis kommen, dass eine Krankheit vorliegt oder eine Person eine gesuchte Verbrecherin bzw. ein gesuchter Verbrecher ist. Die Norm findet deshalb wohl nur auf Klassifizierungen oder Identifikationen durch Gesichtserkennungssysteme Anwendung, nicht aber auf Authentifikationen, da dabei keine Bewertung der Persönlichkeit vorgenommen wird.[70]

---

64 Art. 22 Abs. 2 lit. c) DSGVO.

65 Buchner (Fn. 57), Art. 22 Rn. 34.

66 Buchner (Fn. 57), Art. 22 Rn. 31.

67 Bei einer ausdrücklichen Einwilligung ergibt sich dies in Bezug auf besondere Kategorien personenbezogener Daten aus Art. 22 Abs. 4 DSGVO (Voraussetzung für die Zulässigkeit der automatisierten Einzelentscheidung), im Hinblick auf sonstige personenbezogene Daten aus Art. 22 Abs. 3 DSGVO (lediglich bußgeldbewehrte Pflicht der Verantwortlichen nach Art. 83 Abs. 5 lit. b DSGVO).

68 Vgl. Erwägungsgrund 71 DSGVO.

69 Vgl. Art. 13 Abs. 2 lit. f) DSGVO. Damit korrespondiert auch ein Auskunftsrecht nach Art. 15 Abs. 1 lit. h) DSGVO.

70 So im Ergebnis auch Buchner (Fn. 57), Art. 22 Rn. 17 f. m. w. N.

6 Gesichtserkennung in der Praxis – Fallbeispiele und Empfehlungen

Anhand von Anwendungsfällen der Authentifikation, Klassifizierung und Identifikation wird regulatorischer Handlungsbedarf diskutiert.

6.1 Authentifikation

Eine datenschutzgerechte Ausgestaltung des Einsatzes von Gesichtserkennungssystemen zum Zwecke der Authentifikation ist möglich, wenn die datenschutzrechtlichen Grundsätze der DSGVO bzw. die sie konkretisierenden Normen der DSGVO und des BDSG sowie gegebenenfalls bereichsspezifische Normen beachtet werden. Beispielsweise kann das Entsperren eines Mobiltelefons auf eine freiwillig erteilte Einwilligung der Betroffenen gestützt werden.[71] Für die Passkontrolle durch öffentliche Stellen kommt eine Rechtsgrundlage in Betracht (vgl. den Grundsatz der Rechtmäßigkeit und den Grundsatz von Treu und Glauben).[72] Hierfür dürfen die auf dem elektronischen Speichermedium des Passes gespeicherten biometrischen Daten ausgelesen werden, die benötigten biometrischen Daten beim Passinhaber erhoben und die biometrischen Daten miteinander verglichen werden (vgl. den Grundsatz der Datenminimierung).

Die Verarbeitung der Daten darf nur zu den festgelegten Zwecken erfolgen: Die Betroffenen dürften in der Regel nur für das Entsperren des Mobiltelefons ihre Einwilligung gegeben haben und eine Rechtsgrundlage für die Weiterverwendung der bei einer Passkontrolle erhobenen Daten ist nicht ersichtlich (vgl. den Zweckbindungsgrundsatz). Die Daten sind nach Zweckerreichung wieder zu löschen (vgl. den Grundsatz der Speicherbegrenzung).[73] Die Betroffenen sind in den Beispielsfällen überdies datenschutzgerecht über die Datenverarbeitung zu informieren, insbesondere über die Identität des Verantwortlichen, den Zweck der Verarbeitung, die Kontaktdaten des Datenschutzbeauftragten, ihre Betroffenenrechte sowie ihr Beschwerderecht bei einer Aufsichtsbehörde (vgl. den Grundsatz der Transparenz).[74] Schließlich sind angemessene technische sowie organisatorische Maßnahmen zum Schutz der Sicherheit der Daten vor unbefugter und unrechtmäßiger Verarbeitung, unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder Schädigung einzuführen (vgl. den Grundsatz der Integrität und Vertraulichkeit).[75]

Eine Datenschutzfolgenabschätzung ist durchzuführen.[76]

---

71 Vgl. Art. 9 Abs. 2 lit.a) DSGVO i. V. m. Art. 7 DSGVO.

72 Vgl. § 16a S. 2 Passgesetz.

73 Vgl. Art. 17 DSGVO, § 16a S. 3 Passgesetz.

74 Vgl. Art. 12, 13, 14 DSGVO bzw. das Erfordernis einer informierten Einwilligung.

75 Vgl. Art. 32 DSGVO.

76 Vgl. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Fn. 59), Nr. 1 „Verarbeitung von biometrischen Daten“.

Fazit Die Anwendung von Gesichtserkennung zur Authentifikation wird durch die bestehenden Normen hinreichend geregelt. Gesetzgeberischer Handlungsbedarf ist nicht ersichtlich.

6.2 Klassifizierung

Da Klassifizierung zu Diskriminierung führen kann, gibt es politische Bestrebungen, sie zu regulieren bzw. ausdrücklich zu verbieten.

Regulierungsvorschläge des Europarats[77] sowie des Europäischen Datenschutzausschusses / Europäischen Datenschutzbeauftragten

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 Status einer Person zu bestimmen, solle verboten werden, es sei denn, es sind angemessene Schutzvorkehrungen rechtlich vorgesehen, die jedwedes Risiko einer Diskriminierung vermeiden.

Ebenfalls solle „Affekt-Erkennungstechnologie" verboten werden, die Emotionen erkennen und dazu benutzt werden kann, Persönlichkeitsmerkmale, innere Gefühlszustände, die psychische Gesundheit oder den Grad des Engagements von Arbeitnehmern zu bestimmen. Diese Form der Technologie stelle ein hohes Risiko dar, etwa bei Beschäftigungsverhältnissen, beim Zugang zu Versicherungen und zu einer Ausbildung.

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, wenn sie Individuen kategorisieren kann, sei es nach ihrer ethnischen Herkunft, ihrem Geschlecht, ihrer politischen oder sexuellen Orientierung oder nach anderen diskriminierenden Gründen, die nach Artikel 21 der Europäischen Grundrechtecharta verboten sind.[78]

---

77 Vgl. Council of Europe, Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Guidelines on Facial Recognition, 2021, S. 5, ↗ https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3 [19.07.2021]; vgl. auch Europarat, Pressemitteilung vom 28. Januar 2021, Facial Recognition: Strict Regulation Is Needed to Prevent Human Rights Violations, ↗ https://search.coe.int/directorate_of_communications/Pages/result_details.aspx?ObjectId=0900001680a12f84 [19.07.2021].

78 European Data Protection Board / European Data Protection Supervisor, 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), 2021, S. 12, ↗ https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en [19.07.2021].

Gleichfalls solle Künstliche Intelligenz verboten werden, die Emotionen von Betroffenen erkennen kann, mit Ausnahme im Bereich Gesundheit und Forschung.[79]

Regulierungsvorschläge der EU-Kommission[80]

Anders als der Europarat (und der Europäische Datenschutzausschuss sowie der Europäische Datenschutzbeauftragte) schlägt die EU-Kommission in ihrem am 21. April 2021 veröffentlichten Entwurf zur Regulierung von Künstlicher Intelligenz nicht vor, derartige Gesichtserkennungssysteme zu verbieten.

Solche Gesichtserkennungssysteme können allerdings „Systeme zur biometrischen Kategorisierung" bzw. „Emotionserkennungssysteme" darstellen:

- Ein „System zur biometrischen Kategorisierung" ist ein KI-System, das dem Zweck dient, natürliche Personen auf der Grundlage ihrer biometrischen Daten bestimmten Kategorien wie Geschlecht, Alter, Haarfarbe, Augenfarbe, Tätowierung, ethnische Herkunft oder sexuelle oder politische Ausrichtung zuzuordnen.[81]

- Ein „Emotionserkennungssystem" ist ein KI-System, das dem Zweck dient, Emotionen oder Absichten natürlicher Personen auf der Grundlage ihrer biometrischen Daten festzustellen oder daraus abzuleiten.[82]

Nutzer derartiger Systeme sollen die betroffenen Personen darüber informieren müssen, dass ein solches System eingesetzt wird. Diese Vorgabe gilt nicht für gesetzlich zur Aufdeckung, Verhütung, Ermittlung und Verfolgung von Straftaten zugelassene KI-Systeme, die zur biometrischen Klassifizierung verwendet werden.[83]

Neben dieser Transparenzverpflichtung kann derartige Gesichtserkennung nach den Regulierungsvorschlägen der EU-Kommission eine Künstliche Intelligenz mit hohem Risiko sein, für die bestimmte weitergehende obligatorische Auflagen gelten sollen. Dies hängt davon ab, in welchem Kontext das Gesichtserkennungssystem eingesetzt wird.

Ein hohes Risiko haben nach den Vorschlägen der EU-Kommission KI-Systeme, die in den Bereichen „Allgemeine und berufliche Bildung", „Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit", „Zugänglichkeit und Inanspruchnahme grundlegender priva-

79 European Data Protection Board / European Data Protection Supervisor (Fn. 78), S. 12.

80 Vgl. Europäische Kommission, 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 vom 21.04.2021, ↗ https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0019.02/DOC_1&format=PDF [19.07.2021].

81 Europäische Kommission (Fn. 80), Art. 3 Nr. 35.

82 Europäische Kommission (Fn. 80), Art. 3 Nr. 34.

83 Europäische Kommission (Fn. 80), Art. 52 Abs. 2.

ter und öffentlicher Dienste und Leistungen“, „Strafverfolgung“ sowie „Migration, Asyl und Grenzkontrolle“ eingesetzt werden.[84]

So sollen KI-Maschinen ein hohes Risiko haben, die zum Zugang zur Ausbildung oder zur Arbeit eingesetzt werden sowie dazu, Schülerinnen und Schüler bzw. Studierende oder Arbeitnehmerinnen und Arbeitnehmer bzw. Selbstständige zu bewerten.[85]

Auch KI-Systeme, die die Berechtigung zu öffentlichen Leistungen oder die Kreditwürdigkeit bewerten, sollen nach den Vorschlägen der EU-Kommission ein hohes Risiko darstellen.[86]

Dies soll auch gelten, wenn Strafverfolgungsbehörden KI-Systeme einsetzen zum Zwecke einer Risikoanalyse des Begehens oder Wiederbegehens einer Straftat, zum Zwecke der Bestimmung des emotionalen Zustandes von natürlichen Personen oder zum Profiling im Zuge der Aufdeckung, Ermittlung oder Verfolgung von Straftaten.[87]

Ebenso sollen Systeme als mit hohem Risiko behaftet angesehen werden, die von den zuständigen Behörden im Bereich Migration/Asyl/Grenzkontrolle dazu eingesetzt werden, den emotionalen Zustand von natürlichen Personen zu bestimmen sowie ein Sicherheitsrisiko, ein Risiko irregulärer Einwanderung oder ein Gesundheitsrisiko der betroffenen Personen einzuschätzen.[88]

Folgende obligatorische Auflagen gelten für derartige Gesichtserkennungssysteme mit hohem Risiko, die in einer vorab vorzunehmenden Konformitätsbewertung geprüft und laufend überwacht werden:

Risikomanagementsystem

Risiken eines Systems sollen identifiziert und so weit wie möglich gemindert werden. Verbleibende Risiken sollen kontrolliert werden. Dieses Verfahren erfolgt durch Tests.[89]

Daten und Daten-Governance

Trainings- und Testdatensätze sollen insbesondere relevant, repräsentativ, frei von Fehlern und vollständig sein, damit die Technik nicht diskriminiert.[90]

Technische Dokumentation

Eine technische Dokumentation soll gewährleisten, dass die zuständigen Prüfbehörden überwachen können, dass die obligatorischen Auflagen eingehalten werden.[91]

---

84 Europäische Kommission, 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, ↗ https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0019.02/DOC_2&format=PDF [19.07.2021], Anhang III.

85 Europäische Kommission (Fn. 84), Nr. 3 u. 4 Anhang III.

86 Europäische Kommission (Fn. 84), Nr. 5 Anhang III.

87 Europäische Kommission (Fn. 84), Nr. 6 lit. a), b), e), f) Anhang III.

88 Europäische Kommission (Fn. 84), Nr. 7 lit. a), b) Anhang III.

89 Europäische Kommission (Fn. 80), Artikel 9.

90 Europäische Kommission (Fn. 80), Artikel 10.

91 Europäische Kommission (Fn. 80), Artikel 11.

Aufzeichnungspflichten

Ereignisse während des Betriebs des KI-Systems sollen automatisch aufgezeichnet werden (Logging), um die Funktionsweise der Maschine nachverfolgen zu können.[92]

Transparenz und Bereitstellung von Informationen für die Nutzer

Nutzer sollen transparent über das KI-System informiert werden. Dazu gehören insbesondere Informationen über die Identität und die Kontaktdaten des Anbieters des Systems sowie die Charakteristiken der Maschine, ihre Fähigkeiten und die Grenzen ihrer Leistung.[93]

Menschliche Aufsicht

Um Risiken für die Gesundheit, Sicherheit oder Grundrechte der Betroffenen zu minimieren, soll die Künstliche Intelligenz von Menschen beaufsichtigt werden, während sie angewandt wird.[94]

Genauigkeit, Robustheit und Cybersicherheit

Hochrisiko-KI-Systeme sollen so gestaltet werden, dass sie ein angemessenes Level von Genauigkeit, Robustheit und Cybersicherheit aufweisen.[95]

Stellungnahme

Es ist zutreffend, dass gerade Gesichtserkennungssysteme zur Klassifizierung das Risiko bergen, dass Betroffene diskriminiert werden.

Betroffene könnten allein aufgrund ihrer ethnischen Herkunft, ihrer religiösen oder sonstigen Überzeugung, ihres Geschlechts, ihres Alters, ihrer sexuellen Orientierung oder ihrer politischen Überzeugungen Nachteile erleiden. Auch könnten etwa Arbeitnehmerinnen und Arbeitnehmer oder Schülerinnen und Schüler nachteilig behandelt werden, je nachdem welches Aufmerksamkeitslevel sie zeigen, oder Betroffene diskriminiert werden, wenn sie psychisch nicht gesund sind oder bestimmte Emotionen, wie Aggression, zeigen.

Die Diskriminierungsgefahr besteht also bereits, wenn die Systeme technisch zuverlässig sind. Umso schwerer kann es dann wiegen, wenn die Künstliche Intelligenz technisch unzuverlässig ist und Betroffene fehlerhaft einer bestimmten Kategorie oder Emotion zugewiesen werden, beispielsweise eine Krankheit, ein Aufmerksamkeitslevel oder ein Alter diagnostiziert bekommen, die/das nicht zutrifft.

Andererseits sind auch nützliche Anwendungsfälle im Interesse der Betroffenen denkbar, beispielsweise das korrekte Erkennen von Krankheiten oder das Messen der Aufmerksamkeit von Kraftfahrzeugführern.

---

92 Europäische Kommission (Fn. 80), Artikel 12.

93 Europäische Kommission (Fn. 80), Artikel 13.

94 Europäische Kommission (Fn. 80), Artikel 14.

95 Europäische Kommission (Fn. 80), Artikel 15.

Vor diesem Hintergrund stellt sich die Frage, ob der bereits geltende Rechtsrahmen ausreichend Schutz vor Diskriminierung bietet oder ein Verbot der Technik (Vorschlag Europarat) bzw. weitergehende Vorschriften (Vorschlag Europäische Kommission) notwendig sind.

Zunächst ist zu beachten, dass durch diese Formen von Gesichtserkennung Profiling stattfindet. Profiling ist „jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen“.[96]

Außerdem kann es sich – je nach Fallkonstellation – um die Verarbeitung besonderer Kategorien personenbezogener Daten handeln, beispielsweise über die ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Daten zur sexuellen Orientierung und Gesundheitsdaten.[97]

Profiling und die Verarbeitung besonderer Kategorien personenbezogener Daten ist nach dem datenschutzrechtlichen Verbot mit Erlaubnisvorbehalt grundsätzlich verboten, es sei denn, es gibt eine (enge) gesetzliche Rechtsgrundlage oder die Betroffenen erteilen ihre Einwilligung (vgl. den Grundsatz der Rechtmäßigkeit).

Zunächst kann festgestellt werden, dass eine gesetzliche Rechtsgrundlage für diese Formen der Gesichtserkennung nicht ersichtlich ist. Auch dürfte eine gesetzliche Rechtsgrundlage, die – ohne das Einverständnis der Betroffenen – zur Klassifizierung durch Gesichtserkennungssysteme berechtigt, nicht geschaffen werden können. Der Einsatz der Systeme greift sehr tief in die Persönlichkeit der Betroffenen ein, sodass eine gesetzliche Rechtsgrundlage unverhältnismäßig wäre.

Betroffene Personen müssten also in die Datenverarbeitung durch diese Art der Technologie einwilligen.

Hier gilt es zu beachten, dass die Einwilligung freiwillig erteilt sein muss (vgl. den Grundsatz von Treu und Glauben). Die Betroffenen müssen eine „echte und freie Wahl“ haben.[98] Eine Einwilligung ist dann nicht gültig, „wenn die betroffene Person keine wirkliche Wahl hat, sich zur Einwilligung gedrängt fühlt oder negative Auswirkungen erdulden muss, wenn sie nicht einwilligt“.[99]

Dies ist aufgrund eines bestehenden Ungleichgewichts der Macht regelmäßig zwischen Behörden und Bürgerinnen bzw. Bürgern sowie Arbeitgeberinnen bzw. Arbeitgebern und

96 Vgl. Art. 4 Nr. 4 DSGVO, § 46 Nr. 4 BDSG.

97 Vgl. Art. 9 Abs. 1 DSGVO.

98 Vgl. Erwägungsgrund 42 der DSGVO.

99 Vgl. European Data Protection Board, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, 2020, S. 8, ↗ https://www.datenschutzkonferenz-online.de/media/dsgvo/Leitlinien%2005-2020%20zur%20Einwilligung%20gem%C3%A4%C3%9F%20Verordnung%202016-679.pdf [19.07.2021].

Arbeitnehmerinnen bzw. Arbeitnehmern der Fall.[100] Eine Einwilligung kann dann in der Regel keine gültige Rechtsgrundlage liefern, da sie nicht freiwillig erteilt worden ist.

Ein Ungleichgewicht der Macht kann auch in anderen Fällen bestehen, „in denen Zwang oder Druck ausgeübt wird oder keine Möglichkeit zur Ausübung des freien Willens besteht“[101], sodass eine Einwilligung dann nicht freiwillig wäre und nicht in Betracht kommt.

Eine Einwilligung ist bei bestehendem Machtungleichgewicht nur denkbar, wenn „sich das Ungleichgewicht in der konkreten Einwilligungssituation nicht niederschlägt, etwa weil die Verarbeitung im Interesse des Betroffenen liegt oder der Betroffene keinerlei Nachteile erleidet, wenn er seine Einwilligung verweigert“.[102]

Die Einwilligung muss zudem „in informierter Weise“ erfolgen (vgl. den Grundsatz der Transparenz).[103] Betroffene Personen müssen insbesondere darüber informiert werden, von wem zu welchem Zweck wie lange personenbezogene Daten verarbeitet werden sollen und wer potenzielle Empfänger der Daten sind.

Hinzu kommen die Transparenzanforderungen aus dem Verbot automatisierter Einzelentscheidungen.[104] Betroffene müssen darüber informiert werden, dass eine automatisierte Einzelentscheidung einschließlich Profiling stattfindet. Auch müssen sie über die involvierte Logik, die Tragweite sowie die angestrebten Auswirkungen einer derartigen Verarbeitung unterrichtet werden. Zudem muss die Einwilligung ausdrücklich erfolgen.

Wenn betroffene Personen in Kenntnis all dieser Umstände informiert sind und ausdrücklich einwilligen, so müssen sie in jedem Fall stets die Möglichkeit haben, zu erwirken, dass eine Person in die automatisierte Datenverarbeitung eingreift, sie ihren eigenen Standpunkt darlegen können und sie die automatisierte Entscheidung anfechten können. Sie müssen also stets die Möglichkeit haben, dass doch wieder ein Mensch die Entscheidung inhaltlich verantwortet und dabei auch den Standpunkt der Betroffenen berücksichtigt.[105]

Auch ist eine Datenschutzfolgenabschätzung durchzuführen.[106]

Fazit

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).

---

100 Vgl. Erwägungsgrund 43 der DSGVO; vgl. auch European Data Protection Board (Fn. 99), S. 9 ff.

101 Vgl. European Data Protection Board (Fn. 99), S. 10 f.

102 Stemmer, in: Brink/Wolff, BeckOK Datenschutzrecht, 36. Edition, Stand: 01.05.2021, Art. 7 Rn. 50.

103 Vgl. Art. 4 Nr. 11 DSGVO.

104 Vgl. Art. 13 Abs. 2 lit. f) DSGVO.

105 Vgl. Art. 22 DS-GVO.

106 Vgl. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Fn. 59), Nr. 11 „Einsatz von Künstlicher Intelligenz zur [...] Bewertung persönlicher Aspekte der betroffenen Person“.

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 erforderliche Einwilligung muss freiwillig sein, sodass in Fällen eines Ungleichgewichts der Macht zwischen Verantwortlichen und Betroffenen eine Einwilligung regelmäßig nicht in Betracht kommt. Dies ist insbesondere im Staat-Bürger-Verhältnis sowie zwischen Arbeitgeberinnen bzw. Arbeitgebern und Arbeitnehmerinnen bzw. Arbeitnehmern der Fall.

Es verbleibt eine eng begrenzte Zahl von Fällen, in denen eine Klassifizierung durch Gesichtserkennungssysteme auf Basis einer freiwilligen Einwilligung der Betroffenen zulässig sein kann. Dies sind insbesondere der Bereich Gesundheit, Wissenschaft und die Sicherheit des Straßenverkehrs. Auf Grundlage einer freiwilligen Einwilligung können also enge Anwendungsfälle, wie etwa das Erkennen von Krankheiten, die Kontrolle der Aufmerksamkeit von Kraftfahrzeugführern oder wissenschaftliche Forschung, durchgeführt werden.

In den verbleibenden 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 stets die Möglichkeit haben, dass doch wieder ein Mensch die Entscheidung inhaltlich verantwortet und ihren Standpunkt berücksichtigt. Dies wirkt Diskriminierung durch fehlerhafte Gesichtserkennungssysteme entgegen, die etwa durch nicht repräsentative Datensätze entstehen kann.

Vor diesem Hintergrund scheint der geltende Rechtsrahmen in einem Maße Schutz vor Diskriminierung zu bieten, dass ein vom Europarat bzw. den Europäischen Datenschutzaufsichtsbehörden vorgeschlagenes ausdrückliches gesetzliches Verbot dieser Form der Technologie nicht notwendig sein dürfte. Die Europäischen Datenschutzaufsichtsbehörden sollten jedoch in einer gemeinsamen Stellungnahme die 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 sowie obligatorischen Auflagen unterworfen werden.

Gleichwohl sind all dies Bereiche, in denen ein Einsatz von Gesichtserkennungssystemen 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).

Anzuregen ist deshalb, dass die Europäische Kommission den Bereich „Gesundheit" in ihren Katalog von KI mit hohem Risiko aufnimmt. 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.

6.3 Identifikation

Hoch umstritten und öffentlich breit diskutiert ist der Einsatz von Gesichtserkennungssystemen zur Identifikation.

Clearview und PimEyes

Clearview ist ein US-amerikanisches Unternehmen mit Sitz in New York, das nach Medienberichten eine Datenbank von mehr als drei Milliarden Aufnahmen von Gesichtern besitzt, die es im Internet zusammengesucht hat, insbesondere aus sozialen Netzwerken oder von Unternehmensseiten. Kunden können mittels eines Gesichtserkennungssystems ein Foto mit den gespeicherten Milliarden von Aufnahmen abgleichen und bekommen Suchergebnisse mit Fotos angezeigt, einschließlich der Quelle, beispielsweise von einer Unternehmensseite oder einem sozialen Netzwerk.[107] Kunden von Clearview waren insbesondere Sicherheitsbehörden, die mithilfe des Gesichtserkennungssystems Verdächtige identifizierten.[108] Die *New York Times*, die über Clearview berichtete, sprach von einem „Ende der Privatsphäre".[109]

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit hat nach einer Beschwerde ein Verfahren gegen Clearview eröffnet, die Anwendbarkeit der DSGVO 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 Hamburger Beauftragte für Datenschutz und Informationsfreiheit hat diesbezüglich mitgeteilt,

---

107 Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Tätigkeitsbericht Datenschutz 2020, 2021, S. 105, ↗ https://datenschutz-hamburg.de/assets/pdf/29._taetigkeitsbericht_datenschutz_2020.PDF [19.07.2021].

108 Laufer, Clearview AI verweigert Zusammenarbeit mit deutscher Datenschutzaufsicht, in: netzpolitik.org, 2020, ↗ https://netzpolitik.org/2020/gesichtserkennung-clearview-ai-verweigert-zusammenarbeit-mit-deutscher-datenschutzaufsicht/ [19.07.2021].

109 Köver, EU-Datenschutzregeln schützen nicht vor Gesichter-Suchmaschinen, in: netzpolitik.org, 2020, ↗ https://netzpolitik.org/2020/eu-datenschutzregeln-schuetzen-nicht-vor-gesichter-suchmaschinen/ [19.07.2021].

dass eine solche Anordnung nicht umzusetzen sei, da nicht davon auszugehen sei, dass Clearview Informationen über den gewöhnlichen Wohnort der Betroffenen (in Hamburg) habe.[110] Vier Europäische Bürgerrechtsorganisationen haben mittlerweile ebenfalls eine Beschwerde bei den Datenschutzbehörden von Frankreich, Österreich, Italien, Griechenland und dem Vereinigten Königreich eingereicht.[111]

PimEyes ist ein Unternehmen mit ehemals Sitz in Polen, jetzt auf den Seychellen, das genauso wie Clearview die Identifikation von Personen mittels Gesichtserkennungssystemen anbietet. Der Unterschied zu Clearview: Die Datenbank ist „kleiner", umfasst etwa 900 Millionen Menschen und der Service wird für jedermann, also nicht nur Sicherheitsbehörden angeboten. Netzpolitik.org hat über PimEyes berichtet und spricht von der „Abschaffung der Anonymität".[112] Vor allem besonders schutzbedürftige Gruppen, wie queere Menschen, könnten durch die Software geoutet oder Besucher von Demonstrationen identifiziert werden.[113]

Tankred Schipanski, der digitalpolitische Sprecher der Union im Bundestag, hat das Angebot von PimEyes als „unhaltbar" bezeichnet. „Wenn eine Regulierung auf Ebene der EU zeitnah nicht gelinge, müssen wir hier als nationaler Gesetzgeber tätig werden". Die netzpolitische Sprecherin der Linken im Bundestag, Anke Domscheit-Berg, sagte, PimEyes sei „hochgefährlich". Jens Zimmermann, der digitalpolitische Sprecher der SPD-Fraktion, forderte eine „genaue Prüfung, ob die bestehenden gesetzlichen Regelungen einen ausreichenden Schutz bieten".[114]

Der Baden-Württembergische Landesbeauftragte für Datenschutz hat mittlerweile ein Verfahren gegen PimEyes eröffnet, da auch Bürgerinnen und Bürger aus Baden-Württemberg von der Verarbeitung betroffen sein können.[115]

Stellungnahme

Die Verarbeitung von Fotos durch Clearview und PimEyes von europäischen Bürgerinnen und Bürgern, um diese zu identifizieren, ist datenschutzrechtlich unzulässig, da die Betroffenen darin nicht eingewilligt haben.

---

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

111 Reuter, Datenschutz-Verfahren gegen PimEyes und Clearview, in: netzpolitik.org, 2021, ↗ https://netzpolitik.org/2021/gesichtserkennung-datenschutz-verfahren-gegen-pimeyes-und-clearview/ [19.07.2021]; Krempl, Gesichtserkennung: Europäische Bürgerrechtler gehen gegen Clearview vor, in: heise online, 2021, ↗ https://www.heise.de/news/Gesichtserkennung-Europaeische-Buergerrechtler-gehen-gegen-Clearview-vor-6055056.html [19.07.2021].

112 Dachwitz/Laufer/Meineck, Gesichtserkennung ist eine Waffe, in: netzpolitik.org, 2021, ↗ https://netzpolitik.org/2020/npp-204-pimeyes-gesichtserkennung-ist-eine-waffe/ [19.07.2021].

113 Dachwitz/Laufer/Meineck (Fn. 112).

114 ZDFheute, Gesichtsdatenbank „PimEyes" - „Hochgefährliche" Suchmaschine, 2020, ↗ https://www.zdf.de/nachrichten/digitales/pimeyes-gesichtserkennung-100.html [19.07.2021].

115 Reuter (Fn. 111).

Der räumliche Anwendungsbereich der Datenschutz-Grundverordnung ist eröffnet,[116] auch wenn Clearview seine Niederlassung in den USA und PimEyes auf den Seychellen hat, da Kunden der Unternehmen das Verhalten von Unionsbürgerinnen und Unionsbürgern in der Europäischen Union beobachten können, indem ihnen die entsprechenden Fotos der Betroffenen nach Einsatz des Gesichtserkennungssystems angezeigt werden. Auf den Fotos sind die Betroffenen in ihrem privaten oder beruflichen Umfeld zu erkennen. Für eine Eröffnung des Anwendungsbereichs spricht auch, dass der Gesetzgeber der DSGVO den Betroffenen Schutz sichern wollte, selbst wenn die Verantwortlichen nicht in der Union ansässig sind.[117]

Es handelt sich weiter um eine Verarbeitung von biometrischen Daten, um Gesichtsbilder, die mit speziellen technischen Verfahren gewonnen wurden und die die eindeutige Identifikation der Betroffenen ermöglichen.[118] Die Verarbeitung von biometrischen Daten ist nach dem datenschutzrechtlichen Verbot mit Erlaubnisvorbehalt grundsätzlich verboten, es sei denn, es liegt eine gesetzliche Rechtsgrundlage vor oder die Betroffenen haben eingewilligt.[119] Da weder eine gesetzliche Rechtsgrundlage ersichtlich ist, noch die betroffenen Personen eingewilligt haben, ist die Datenverarbeitung verboten.

Fazit

Die Verarbeitung von biometrischen Daten von Bürgerinnen und Bürgern der Europäischen Union durch Clearview und PimEyes ist bereits nach geltendem Recht verboten. Gleichwohl zeigt sich am Beispiel Clearview, dass ein Problem der Durchsetzung des geltenden Rechts zu bestehen scheint.

Hintergrund dürfte zum einen sein, dass eine Anordnung auf Löschung aller personenbezogenen Daten von EU-Bürgerinnen und -Bürgern daran scheitern dürfte, dass das Unternehmen nicht feststellen könnte, wer auf den gespeicherten Fotos Unionsbürgerinnen und Unionsbürger sind.

Auch stellen sich Fragen der Durchsetzbarkeit des Rechts gegenüber Unternehmen mit Sitz im Ausland.

Hier ist wohl der Gesetzgeber gefragt, gemeinsam mit den Datenschutzaufsichtsbehörden über Wege und Mittel zur Durchsetzung des geltenden Rechts zu beraten. Gegebenenfalls bedarf es weiterer (bilateraler) völkerrechtlicher Verträge der EU mit Drittstaaten, um die personenbezogenen Daten von EU-Bürgerinnen und -Bürgern zu schützen.

116 Vgl. Art. 3 Abs. 2 lit. b) DSGVO.

117 Vgl. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit (Fn. 107), S. 106.

118 Es ist wohl davon auszugehen, dass die Gesichtsbilder „mit speziellen technischen Verfahren“ gewonnen wurden; auch lässt eine geringe Fehlerrate bei Anwendung der Gesichtserkennungssoftware das Kriterium der „Eindeutigkeit“ wohl nicht entfallen.

119 Vgl. Art. 9 Abs. 2 DSGVO.

Biometrische Gesichtserkennung im öffentlichen Raum[120]

Bekannt ist biometrische Gesichtserkennung im öffentlichen Raum vor allem durch den Test am Bahnhof Berlin Südkreuz in den Jahren 2017 und 2018. Bei biometrischer Gesichtserkennung im öffentlichen Raum werden alle Bürgerinnen und Bürger im Anwendungsfeld der Videokameras „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.

Europäische Regulierungsbestrebungen

D ie EU-Kommission hat zunächst ein Verbot dieser Form von Gesichtserkennung im öffentlichen Raum für die nächsten fünf Jahre erwogen.[121] In ihrem im Februar 2020 veröffentlichten *Weißbuch Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen* rückte sie aber davon ab und hat nun lediglich vorgeschlagen, dass die Technik „ausnahmslos als mit hohem Risiko behaftet angesehen" und obligatorischen strikten Auflagen unterworfen werden solle, die in einer vorab vorzunehmenden Konformitätsbewertung überprüft und kontinuierlich überwacht werden sollen.[122]

In ihren am 21. April 2021 veröffentlichten Regulierungsvorschlägen zu Künstlicher Intelligenz geht die Europäische Kommission nun einen Mittelweg: 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:[123]

- 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

---

120 Auch „biometrische Fernidentifikation", „intelligente Videoüberwachung" oder „Videoüberwachung mit biometrischer Gesichtserkennung" genannt.

121 Fanta, Künstliche Intelligenz - EU erwägt Verbot von Gesichtserkennung, in: netzpolitik.org, 2020, ↗ https://netzpolitik.org/2020/eu-erwaegt-verbot-von-gesichtserkennung/ [19.07.2021].

122 Europäische Kommission, Weißbuch, Zur Künstlichen Intelligenz - Ein europäisches Konzept für Exzellenz und Vertrauen, 2020, S. 21 ff., ↗ https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_de.pdf [19.07.2021].

123 Europäische Kommission (Fn. 80), Art. 5 Abs. 1 lit. d).

– 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.

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, wahrscheinlich und in welchem Ausmaß der Schaden wiegen würde, 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 welches Ausmaß sie haben.[124] 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.[125]

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 beginnen können und die Genehmigung soll während oder nach dem Einsatz der Technik eingeholt 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.[126]

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.[127]

Auch soll biometrische Gesichtserkennung im öffentlichen Raum als eine Technologie mit hohem Risiko eingestuft werden, für welche obligatorische Auflagen gelten, die in einem Konformitätsbewertungsverfahren geprüft und laufend überwacht werden.[128]

---

124 Europäische Kommission (Fn. 80), Art. 5 Abs. 2.

125 Europäische Kommission (Fn. 80), Art. 5 Abs. 2.

126 Europäische Kommission (Fn. 80), Art. 5 Abs. 3.

127 Europäische Kommission (Fn. 80), Art. 5 Abs. 4.

128 Europäische Kommission (Fn. 84), Anhang III.

Selbst wenn die EU-Regulierungsvorschläge Gesetz würden, bedürfte es demnach noch einer nationalen Rechtsgrundlage für ihren Einsatz, die biometrische Gesichtserkennung im öffentlichen Raum erlaubt. Die Europäische Kommission gibt insofern lediglich einen Rahmen vor, innerhalb dessen der nationale Gesetzgeber eine Rechtsgrundlage schaffen kann:

„Folglich steht es den Mitgliedstaaten frei, eine solche Möglichkeit generell oder nur in Bezug auf einige der in dieser Verordnung genannten Ziele, für die eine genehmigte Verwendung gerechtfertigt werden kann, vorzusehen".[129]

Der Europäische Datenschutzausschuss und der Europäische Datenschutzbeauftragte empfehlen hingegen in einer gemeinsamen Stellungnahme vom 18. Juni 2021, dass die biometrische Gesichtserkennung im öffentlichen Raum gänzlich verboten werden sollte. Insbesondere habe die Technik unumkehrbare und schwere Auswirkungen auf die (vernünftige) Erwartung der Bevölkerung, sich anonym in der Öffentlichkeit zu bewegen, was auch negative Effekte auf die Ausübung von Meinungsfreiheit, Versammlungsfreiheit und Bewegungsfreiheit hat.[130]

Stellungnahme

Die Europäische Kommission versucht mit ihren Regulierungsvorschlägen ersichtlich einen Mittelweg zwischen dem Verbot der Technologie und ihrer uneingeschränkten Erlaubnis zu gehen. Die Technik wird grundsätzlich verboten und darf nur ausnahmsweise vom nationalen Gesetzgeber erlaubt werden. Die Europäische Kommission gibt einen engen Rahmen vor, innerhalb dessen der nationale Gesetzgeber biometrische Gesichtserkennung im öffentlichen Raum auf Basis einer nationalen Rechtsgrundlage erlauben darf.

Damit einhergehend stuft die Europäische Kommission biometrische Gesichtserkennung im öffentlichen Raum als KI mit hohem Risiko ein, die strikten Auflagen unterliegt. Sie soll in einem vorab vorzunehmenden Konformitätsbewertungsverfahren ex ante überwacht und ex post kontrolliert werden.

Dies ist nachvollziehbar. Biometrische Gesichtserkennung im öffentlichen Raum birgt hohe Risiken für die Rechte und Freiheiten der Bürgerinnen und Bürger, insbesondere in Bezug auf ihre Privatsphäre, ihre personenbezogenen Daten sowie ihr Recht auf Nichtdiskriminierung. Diese Risiken sollten durch enge Ausnahmevorschriften und strikte Auflagen möglichst gemindert werden.

Die EU-Kommission verfolgt damit einen risikobasierten Regulierungsansatz.[131] Dieser entspricht dem Grundsatz der Verhältnismäßigkeit,[132] indem er Systeme mit hohem Risiko für die Rechte und Freiheiten der Bevölkerung eingriffsintensiveren Auflagen aussetzt, als sie für sonstige Anwendungen gelten. Dieser wurde auch von der durch die Europäische Kommis-

129 Europäische Kommission (Fn. 80), Erwägungsgrund 22.

130 European Data Protection Board/European Data Protection Supervisor (Fn. 78), S. 11f.

131 Vgl. Europäische Kommission (Fn. 122), S. 20.

132 So auch die EU-Kommission: Vgl. Europäische Kommission (Fn. 122), S. 20.

sion eingesetzten High-Level Expert Group on Artificial Intelligence sowie von der durch die deutsche Bundesregierung eingesetzten Datenethikkommission im Grundsatz als Regulierungsrahmen für Künstliche Intelligenz vorgeschlagen.[133]

Fazit

Die EU-Kommission gibt in ihren Regulierungsvorschlägen einen Rahmen vor, innerhalb dessen der nationale Gesetzgeber biometrische Gesichtserkennung auf Basis einer Rechtsgrundlage erlauben darf.

Es stellt sich damit die Frage, ob es auf nationaler Ebene bereits eine solche Rechtsgrundlage gibt.

Auch lässt sich fragen, ob der Gesetzgeber eine derartige Rechtsgrundlage schaffen könnte, die auch den verfassungsrechtlichen Anforderungen genügt. Denn da die Europäische Kommission nur einen Rahmen für eine nationale Rechtsgrundlage vorgeben möchte, sind ebenfalls gegebenenfalls strengere verfassungsrechtliche Anforderungen zu beachten.

Nationale Regulierungsbestrebungen

Der Test am Bahnhof Berlin Südkreuz wurde auf eine datenschutzrechtliche Einwilligung von Freiwilligen gestützt. Umstritten ist, ob für den regulären Einsatz derartiger Systeme durch die Bundespolizei derzeit eine Rechtsgrundlage besteht.[134]

Nach einer Entschließung der Datenschutzkonferenz, der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, gibt es derzeit keine Rechtsgrundlage für den Einsatz von Videokameras zur biometrischen Gesichtserkennung. Aufgrund der Schwere des Grundrechtseingriffes seien die verfassungsrechtlichen Anforderungen an die Bestimmtheit bestehender Normen nicht erfüllt. Diese erlaubten nur reine Bildaufnahmen bzw. Bildaufzeichnungen durch Videokameras, nicht aber eine Identifikation von betroffenen Personen.[135]

Ebenfalls umstritten ist, ob eine Rechtsgrundlage geschaffen werden kann, die den verfassungsrechtlichen Anforderungen genügt.

Nach Ansicht der Datenschutzkonferenz müsste bei einer entsprechenden Befugnis der Wesensgehalt des Rechts auf informationelle Selbstbestimmung gewahrt bleiben und an-

---

133 High-Level Expert Group on Artificial Intelligence, Policy and Investment Recommendation for Trustworthy AI, 2019, S. 37 f., ↗ https://digital-strategy.ec.europa.eu/en/library/policy-and-investment-recommendations-trustworthy-artificial-intelligence [19.07.2021]; Datenethikkommission der Bundesregierung, Gutachten der Datenethikkommission der Bundesregierung, 2019, S. 173 ff., ↗ https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=6 [19.07.2021].

134 Vgl. Wissenschaftlicher Dienst des Bundestages, Sachstand - Rechtsgrundlage für den Einsatz sog. intelligenter Videoüberwachung durch die Bundespolizei, 2016, ↗ https://www.bundestag.de/resource/blob/439670/e2efe42f49749393cc701c7c4f9af7d8/wd-3-202-16-pdf-data.pdf [19.07.2021].

135 Vgl. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, Entschließung: Einsatz von Videokameras zur biometrischen Gesichtserkennung birgt erhebliche Risiken, 2017, S. 2, ↗ https://www.datenschutzkonferenz-online.de/media/en/20170330_en_gesichtserkennung.pdf [19.07.2021].

gemessene und spezifische Regelungen zum Schutz der Grundrechte und -freiheiten der Betroffenen vorgesehen werden.[136]

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit bezweifelt, ob eine verfassungsmäßige Rechtsgrundlage geschaffen werden könnte, da die Technik erhebliche Einschüchterungseffekte auf Bürgerinnen und Bürger haben könnte, wenn man befürchten müsse, bei Ausübung seiner Meinungs- oder Versammlungsfreiheit identifiziert zu werden.[137]

Auch der Deutsche Anwaltverein hält es für zweifelhaft, ob eine Rechtsgrundlage geschaffen werden kann, die den Vorgaben des Bundesverfassungsgerichts entspricht: „Wenn massenhaft Gesichter von unbescholtenen Bürgerinnen und Bürgern an Bahnhöfen und Flughäfen gescannt werden, dann liegt darin ein schwerer Grundrechtseingriff [...] Ein Scannen dieses Ausmaßes führe zu einem nicht hinnehmbaren Gefühl des Überwachtwerdens und der Einschüchterung".[138]

Bestrebungen, eine Rechtsgrundlage für den Einsatz 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 abgleichen" könne. In einem späteren Entwurf ist dieser Passus gestrichen.[139]

Das Bundesinnenministerium geht jedoch weiter davon aus, dass man rechtlich „auf festem Boden stehe", aber es um Fragen der „gesellschaftlichen Akzeptanz" gehe.[140] Eine Abkehr von den Plänen zur biometrischen Gesichtserkennung habe nicht stattgefunden, auch nachdem auf die Schaffung einer derartigen Rechtsgrundlage im Bundespolizeigesetz vorerst verzichtet wurde.[141]

In der rechtswissenschaftlichen Literatur wird vertreten, dass es derzeit keine Rechtsgrundlage für die Videoüberwachung zur biometrischen Gesichtserkennung gibt.[142] Allerdings wird

136 Vgl. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Fn. 135), S. 3.

137 „fragwürdig": Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, Testimonial iRd. Initiative „Gesichtserkennung stoppen", ↗ https://www.gesichtserkennung-stoppen.de/#testimonials [19.07.2021].

138 Deutscher Anwaltverein, Pressemitteilung PM 01/2020 vom 07.01.2020: Deutscher Anwaltverein warnt vor systematischer Videoüberwachung mit Gesichtserkennung, ↗ https://anwaltverein.de/de/newsroom/pm-01-20-dav-warnt-vor-systematischer-videoueberwachung-mit-gesichtserkennung [19.07.2021].

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

140 Vgl. Bubrowski/Lohse, Gesetzesreform: Warum hat Seehofer die Gesichtserkennung gestoppt?, in: Faz.net, 2020, ↗ https://www.faz.net/aktuell/politik/inland/gesetzesreform-warum-hat-seehofer-die-gesichtserkennung-gestoppt-16599260.html [19.07.2021].

141 Vgl. LTO, Neues Bundespolizeigesetz – Seehofer verzichtet auf Gesichtserkennungssoftware, 2020, ↗ https://www.lto.de/recht/nachrichten/n/entwurf-bundespolizeigesetz-kein-einsatz-software-gesichtserkennung-seehofer/ [19.07.2021].

142 Vgl. etwa Held, MMR 2019, S. 285 (287); vgl. zum weiteren Meinungsstand in der Literatur: Wissenschaftlicher Dienst des Bundestages (Fn. 134).

auch vertreten, dass die Videoüberwachung mit biometrischer Gesichtserkennung auf Basis einer Rechtsgrundlage innerhalb enger verfassungsrechtlicher Grenzen zulässig sein kann.[143]

Stellungnahme

Derzeit ist keine Rechtsgrundlage für den Einsatz von Videokameras zur biometrischen Gesichtserkennung auf Bundesebene ersichtlich. Bestehende Rechtsgrundlagen sind angesichts der Schwere des Grundrechtseingriffs nicht bestimmt und normenklar genug, um eine Videoüberwachung mit biometrischer Gesichtserkennung zu erlauben. Bestehende Ermächtigungsgrundlagen normieren lediglich Bildaufnahmen bzw. Bildaufzeichnungen.

Zwischenfazit

Derzeit gibt es keine gesetzliche Rechtsgrundlage für biometrische Gesichtserkennung mittels Videoüberwachung auf Bundesebene. Damit ist der Einsatz der Technologie nach dem datenschutzrechtlichen Verbot mit Erlaubnisvorbehalt derzeit verboten. Die Frage, die sich stellt, ist: Darf und soll man die Systeme erlauben?

Wäre es verfassungsrechtlich möglich, eine Rechtsgrundlage zu schaffen?

Grundsätzlich gilt, dass der Staat eine Schutzpflicht[144] für seine Bürgerinnen und Bürger hat. Allerdings muss er eine angemessene Balance mit ihrer Freiheit finden. Seine Schutzpflicht findet ihre Grenze deshalb insbesondere in dem Grundsatz der Verhältnismäßigkeit, d. h. in dem Verbot unangemessener Grundrechtseingriffe.[145] „Nicht alles, was technisch an Überwachung und Beschränkung möglich ist, ist verfassungsrechtlich auch erlaubt. Es gibt auch kein verfassungsrechtliches ‚Super-Grundrecht' auf Sicherheit, dem sich alle Freiheitsverbürgungen unterzuordnen hätten".[146]

Das Bundesverfassungsgericht hat diese Balance zwischen Freiheit und Sicherheit für bestimmte staatliche Überwachungsmaßnahmen bereits festgelegt. Um die Rechtmäßigkeit der biometrischen Gesichtserkennung mittels Videoüberwachung zu beurteilen, bietet es sich an, insbesondere die Rechtsprechung des Bundesverfassungsgerichts zur Kfz-Kennzeichenkontrolle[147] heranzuziehen, die innerhalb bestimmter verfassungsrechtlicher Grenzen zulässig ist. Den Urteilen lag der Fall zugrunde, dass Kfz-Kennzeichen mit einer Videokamera

143 Vgl. Thiel, ZPR 2016, S. 218 (221): „jedenfalls keine grundsätzlichen verfassungsrechtlichen Bedenken"; Kulick, NVwZ 2020, S. 1622 (1627): „Landes- oder bundesgesetzliche Regelungen, die sich auf Maßnahmen zur Gesichtserkennung zulässigerweise stützen vermögen, müssen daher hohe verfassungsrechtliche Hürden überwinden"; Hornung/Schindler, ZD 2017, S. 203 (208): „Grundsätzlich darf der Gesetzgeber den Einsatz von Videoüberwachung i. V. m. Gesichtserkennung zur Personenfahndung nur unter sehr engen Voraussetzungen zulassen"; Petri, GSZ 2018, S. 144 (147): „nicht per se unzulässig".

144 Art. 2 II 1 i.V.m. Art. 1 I 2 GG.

145 Papier, NJW 2017, S. 3025 (3030) m. w. N. auf die Rechtsprechung des Bundesverfassungsgerichts.

146 Papier (Fn. 145), S. 3030 m. w. N. auf die Rechtsprechung des Bundesverfassungsgerichts.

147 BVerfG MMR 2008, 308 - Kennzeichen I; BVerfG NJW 2019, 827 - Kennzeichen II.

optisch erfasst, mittels einer Software ausgelesen und mit polizeilichen Fahndungsdatenbanken abgeglichen wurden, sodass Parallelen zur biometrischen Gesichtserkennung mithilfe von Videokameras bestehen. Dabei sollte aber berücksichtigt werden, dass es sich bei biometrischer Videoüberwachung um eine eingriffsintensivere Maßnahme handelt, da das höchstpersönliche Merkmal Gesicht erfasst wird, sodass 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" und der „Online-Durchsuchung" liegen, weshalb ebenfalls die Rechtsprechung des Bundesverfassungsgerichts zu diesen Fahndungsmaßnahmen[148] herangezogen wird. 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.

Zunächst ist der Schutzbereich des Rechtes auf informationelle Selbstbestimmung eröffnet. Denn es schützt Bürgerinnen und Bürger vor einer unbegrenzten Erhebung, Speicherung, Verwendung und Weitergabe ihrer persönlichen Daten und davor, dass sie sich in der Öffentlichkeit gänzlich nicht mehr anonym bewegen können. Das Bundesverfassungsgericht führt diesbezüglich aus: „Zur Freiheitlichkeit des Gemeinwesens gehört es, dass sich die Bürgerinnen und Bürger grundsätzlich fortbewegen können, ohne dabei beliebig staatlich registriert zu werden, hinsichtlich ihrer Rechtschaffenheit Rechenschaft ablegen zu müssen und dem Gefühl eines ständigen Überwachtwerdens ausgesetzt zu sein. Jederzeit an jeder Stelle unbemerkt registriert und daraufhin überprüft zu werden, ob man auf irgendeiner Fahndungsliste steht oder sonst in einem Datenbestand erfasst ist, wäre damit unvereinbar. Vielmehr bedürfen solche Maßnahmen vor der Freiheit des Einzelnen eines spezifischen Grundes und sind als Eingriffe in das Grundrecht auf informationelle Selbstbestimmung rechtfertigungsbedürftig".[149]

Dabei liegt ein rechtfertigungsbedürftiger Eingriff in das Recht auf informationelle Selbstbestimmung auch dann vor, wenn es in einem Fahndungsdatenbestand zu einem Nichttreffer kommt, denn: „Die Einbeziehung der Daten auch von Personen, deren Abgleich letztlich zu Nichttreffern führt, erfolgt nicht ungezielt und allein technikbedingt, sondern ist notwendiger und gewollter Teil der Kontrolle und gibt ihr als Fahndungsmaßnahme erst ihren Sinn".[150]

Der Eingriff darf nur aufgrund eines Gesetzes erfolgen, das verhältnismäßig ist, den Grundsätzen der Normenbestimmtheit und Normenklarheit entspricht und hinreichende organisatorische und verfahrensrechtliche Schutzvorkehrungen aufweist.

Ein verhältnismäßiges Gesetz müsste insbesondere verhältnismäßig im engeren Sinne sein, d. h. die Schwere des Eingriffs darf bei einer Gesamtabwägung nicht außer Verhältnis zum Gewicht der ihn tragenden Gründe stehen.

---

148 BVerfG NJW 2006, 1939 - Rasterfahndung; BVerfG NJW 2008,822 - Online-Durchsuchung.

149 BVerfG NJW 2019, 827 (830) - Kennzeichen II.

150 BVerfG NJW 2019, 827 (829 f.) - Kennzeichen II.

Die Schwere eines Eingriffes bestimmt sich zum einen danach, welche Persönlichkeitsrelevanz die erhobenen Daten aufweisen.[151] Das Bundesverfassungsgericht nennt das Gesicht ein „höchstpersönliches Merkmal".[152] Dies spricht für einen schweren Grundrechtseingriff. Es handelt sich nämlich um besondere Kategorien personenbezogener Daten, um biometrische Daten.[153]

Auch spielt es für die Schwere eines Eingriffs eine Rolle, ob die Bürgerinnen und Bürger durch ihr Verhalten einen Anlass für die Maßnahme gegeben haben oder ob sie anlasslos erfolgen soll, also jeden treffen kann.[154] Die biometrische Gesichtserkennung mittels Videoüberwachung kann jede Bürgerin und jeden Bürger im Anwendungsfeld der Technik treffen. Auch dies spricht für die Schwere des Eingriffs, denn anlasslose Maßnahmen sind von höherer Eingriffsintensität als solche mit Anlass.[155]

Auch für die Schwere des Eingriffs spricht, dass Personen in größerer Anzahl ohne zurechenbaren Anlass von der Maßnahme betroffen sind. Dies kann dazu führen, dass „ein Gefühl des Überwachtwerdens" entsteht und Einschüchterungseffekte eintreten, was sich ebenfalls auf das Gewicht des Eingriffs auswirkt.[156] Bürgerinnen und Bürger könnten ihr Verhalten ändern, ausweichen und grundrechtlich geschützte Verhaltensweisen vermeiden. Diese Gefahr wird vom Bundesverfassungsgericht wie folgt beschrieben: „Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, dass etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert und dass ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlich demokratischen Gemeinwesens ist".[157]

Das Gewicht des Eingriffs bestimmt sich zudem danach, welche Nachteile den Betroffenen aufgrund des Eingriffs drohen können.[158] Die von biometrischer Gesichtserkennung im öffentlichen Raum betroffenen Personen könnten zum Gegenstand staatlicher Ermittlungsmaßnahmen werden.

Dem Eingriff nimmt es aber an Gewicht, wenn Kontrollen im öffentlichen Raum durchgeführt werden und Nichttrefferfälle sofort wieder gelöscht werden, wie dies bei der biometrischen Gesichtserkennung mit Videoüberwachung der Fall wäre.[159]

---

151 BVerfG MMR 2008, 308 (309) - Kennzeichen I.

152 BVerfG NJW 2019, 827 (830) - Kennzeichen II.

153 Vgl. zur Erfassung von besonderen Kategorien personenbezogener Daten: BVerfG NJW 2006, 1939 (1942) - Rasterfahndung.

154 BVerfG MMR 2008, 308 (309) - Kennzeichen I; BVerfG NJW 2006, 1939 (1950) - Rasterfahndung.

155 BVerfG MMR 2008, 308 (309) - Kennzeichen I.

156 BVerfG MMR 2008, 308 (309) - Kennzeichen I; BVerfG NJW 2006, 1939 (1950) - Rasterfahndung.

157 Grundlegend BVerfG NJW 1984, 419 (422) - Volkszählungsurteil.

158 BVerfG NJW 2006, 1939 (1943) - Rasterfahndung.

159 BVerfG NJW 2019, 827 (834) - Kennzeichen II.

Insgesamt ist jedoch von einem schweren Grundrechtseingriff bei Videoüberwachung mittels biometrischer Gesichtserkennung auszugehen, der über eine KfZ-Kennzeichenkontrolle hinausgeht und am ehesten mit einer „Rasterfahndung“ sowie einer „Online-Durchsuchung“ vergleichbar ist.

Das Bundesverfassungsgericht hat bereits in seinen Urteilen zur automatisierten Erfassung von Kfz-Kennzeichen ausgeführt, dass der dortige Eingriff nur dann verhältnismäßig im engeren Sinne ist, wenn die Gründe für den Eingriff ein bestimmtes Gewicht aufweisen.

Konkret führt das Bundesverfassungsgericht aus, dass solche Eingriffe nicht anlasslos oder flächendeckend durchgeführt werden dürfen.[160] „Die Durchführung von Kontrollen zu beliebiger Zeit und an beliebigem Ort ins Blaue hinein ist mit dem Rechtsstaatsprinzip grundsätzlich unvereinbar“.[161] Dies muss erst recht für die biometrische Gesichtserkennung im öffentlichen Raum gelten. Es bedarf also stets eines Anlasses, d. h. eines Grundes und einer Einschränkung der Zeit und Örtlichkeit der Maßnahme.

Zum Grund der Maßnahme: Aufgrund des mit einer „Rasterfahndung“ und einer „Online-Durchsuchung“ am ehesten vergleichbaren Eingriffsgewichts der biometrischen Gesichtserkennung mit Videokameras dürfte Voraussetzung für deren Einsatz stets eine konkrete Gefahr für ein hochrangiges Rechtsgut sein, wie Leib, Leben, Freiheit der Person oder der Bestand und die Sicherheit des Bundes oder der Länder.[162] Auch dürfte die Maßnahme zur Aufklärung besonders schwerer Straftaten[163] zulässig sein. Erforderlich ist stets ein Grund, der auf einer hinreichenden Tatsachenbasis beruht.[164] Lediglich typisierte Gefahrenlagen, also abstrakte Gefahren, dürften im Gegensatz zur Erfassung von Kfz-Kennzeichen aufgrund der Schwere des Eingriffs („höchstpersönliches Merkmal“ Gesicht) bei der Videoüberwachung mittels biometrischer Gesichtserkennung nicht genügen.

Zur Zeit und Örtlichkeit der Maßnahme: Ebenfalls aufgrund der Schwere des Eingriffs dürften Kontrollen wohl nur an eng bestimmten öffentlich zugänglichen Orten wie Verkehrsknotenpunkten, beispielsweise Bahnhöfen oder Flughäfen, durchgeführt werden, an denen aufgrund tatsächlicher Anhaltspunkte mit dem Auffinden der gesuchten Personen zu rechnen ist. Die Maßnahme darf wohl nur so lange andauern, wie aufgrund tatsächlicher Anhaltspunkte die konkrete Gefahrenlage für die erheblichen Rechtsgüter besteht oder mit der Aufklärung der besonders schweren Straftaten zu rechnen ist.

Neben der Verhältnismäßigkeit ist Voraussetzung, dass eine Rechtsgrundlage normenklar und bestimmt gefasst ist. Der Anlass, der Zweck und die Grenzen des Eingriffs müssen in der Ermächtigung bereichsspezifisch, präzise und normenklar festgelegt werden.

Zudem sind organisatorische und verfahrensrechtliche Schutzvorkehrungen zu treffen, um Missbrauchsmöglichkeiten auszuschließen. Aufgrund der Schwere des Eingriffs dürfte ein

160 BVerfG MMR 2008, 308 (314) - Kennzeichen I.

161 BVerfG NJW 2019, 827 (834) - Kennzeichen II.

162 BVerfG NJW 2006, 1939 (1942) - Rasterfahndung; BVerfG NJW 2008, 822 (831) - Online-Durchsuchung.

163 Für die Online-Durchsuchung: § 100b Abs. 2 StPO.

164 Vgl. bereits für die KfZ-Kennzeichen-Kontrolle: BVerfG NJW 2019, 827 (834) - Kennzeichen II.

Richtervorbehalt erforderlich sein.[165] Auch ist der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit zu beteiligen, damit er seine Kontrollbefugnisse ausüben kann. Betroffene sind über die Datenverarbeitung aufzuklären und ihnen ist grundsätzlich Auskunft über gespeicherte Daten zu gewähren. Auch sind zur Zweckerreichung nicht (mehr) erforderliche Daten zu löschen. Die Verwendung der Daten muss auf den gesetzlich bestimmten Erhebungszweck begrenzt sein.[166] Daneben ist ein hohes Maß an Datensicherheit zum Schutz der personenbezogenen Daten notwendig.[167]

Beispielsweise dürfte die Maßnahme auf Basis einer normenklaren und bestimmten Rechtsgrundlage bei konkreten Anhaltspunkten für einen terroristischen Anschlag bzw. nach einem solchen Anschlag an Bahnhöfen oder Flughäfen durchgeführt werden, an denen mit dem Auffinden der gesuchten Personen zu rechnen ist, solange die Gefahrenlage besteht bzw. es die Aufklärung der besonders schweren Straftat erfordert und dort mit dem Auffinden der gesuchten Personen zu rechnen ist. Ein Richter muss die Maßnahme genehmigt haben und der Bundesbeauftragte für den Datenschutz muss seine Kontrollbefugnisse ausüben können. Die erhobenen Daten dürfen nicht für andere Zwecke weiterverwendet werden und sind nach Zweckerreichung zu löschen. Ein hohes Maß an Datensicherheit ist erforderlich.

Darüber hinaus dürfte verfassungsrechtlich eine „Überwachungs-Gesamtrechnung“[168] erforderlich sein. Das Bundesverfassungsgericht hat in seinem Urteil zur Vorratsdatenspeicherung[169] festgestellt, dass alle Überwachungsmaßnahmen zusammengenommen nicht dazu führen dürfen, dass praktisch alle Aktivitäten der Bürgerinnen und Bürger erfasst und registriert werden: „Dass die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf, gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland“.[170]

Es ist deshalb eine „doppelte Verhältnismäßigkeitsprüfung“[171] notwendig: Zum einen die oben dargestellte Verhältnismäßigkeitsprüfung der konkreten Maßnahme Videoüberwachung mit biometrischer Gesichtserkennung. Zum anderen ist zu prüfen, ob alle staatlichen Überwachungsmaßnahmen zusammengenommen zu einer unverhältnismäßigen Belastung der freiheitlichen Rechte der Bürgerinnen und Bürger führen.

Diese Überwachungs-Gesamtrechnung hat der Gesetzgeber durchzuführen, wenn er gedenkt, eine Rechtsgrundlage für die biometrische Gesichtserkennung mittels Videoüberwachung zu schaffen. Es bietet sich an, hierzu wissenschaftliche Untersuchungen zurate zu ziehen. Das Max-Planck-Institut zur Erforschung von Kriminalität, Sicherheit und Recht führt derzeit im Auftrag der Friedrich-Naumann-Stiftung eine Studie zur „Entwicklung eines perio-

---

165 Vgl. zur Online-Durchsuchung: BVerfG NJW 2008, 822 (832).

166 Grundlegend BVerfG NJW 1984, 419 (422) - Volkszählungsurteil.

167 Vgl. BVerfG MMR 2010, 356 (364) - Vorratsdatenspeicherung: Zu Art. 10 GG, die Erwägungen lassen sich wohl aber auf schwere Eingriffe in das Recht auf informationelle Selbstbestimmung übertragen.

168 Roßnagel, NJW 2010, S. 1238.

169 BVerfG NJW 2010, 833 - Vorratsdatenspeicherung.

170 BVerfG NJW 2010, 833 (839) - Vorratsdatenspeicherung.

171 Roßnagel (Fn. 168), S. 1240.

dischen Überwachungsbarometers für Deutschland“ durch.[172] Die Studie kann dem Gesetzgeber als Grundlage für eine Überwachungs-Gesamtrechnung dienen.

Zwischenfazit

Im Ergebnis darf der Gesetzgeber wohl 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“.[173]

  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[174] oder die Produktpiraterie[175] 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-

172 Vgl. Poscher/Kilchling, Pilotprojekt zur Entwicklung eines periodischen Überwachungsbarometers für Deutschland durch das Max-Planck-Institut zur Erforschung von Kriminalität, Sicherheit und Recht, 2021, ↗ https://www.freiheit.org/sites/default/files/2021-03/uberwachungsbarometer_sachstandsbericht_rev_feb2021_final.pdf [19.07.2021].

173 Europäische Kommission (Fn. 80), Erwägungsgrund 9.

174 § 263 Abs. 1 StGB.

175 § 143 Abs. 1 MarkenG.

Durchsuchung“ dürfte die Technologie verfassungsrechtlich wohl ebenfalls nur zur Aufklärung besonders schwerer Straftaten[176] 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 nationale Gesetzgeber die Technik innerhalb sehr enger rechtlicher Grenzen erlauben darf, stellt sich die Frage, ob der nationale Gesetzgeber dies auch tun sollte. Er sollte dies wohl nur tun, wenn unsere Gesellschaft die Technologie auch will. Dies ist eine Frage der gesellschaftlichen Akzeptanz.

Demokratische Debatte

Ob unsere Gesellschaft die Technik auch will, scheint nicht eindeutig zu sein. Ein erstes Stimmungsbild lieferten die Antworten auf die Konsultation der EU-Kommission zum Weißbuch für Künstliche Intelligenz. Danach sprachen sich 28 % der Beteiligten für ein Verbot der Technologie aus. 29 % forderten eine spezifische EU-Regulierung, bevor solche Systeme im öffentlichen Raum eingesetzt werden dürfen. 20 % wollten mehr Anforderungen für die biometrische Gesichtserkennung im öffentlichen Raum. Lediglich 6 % antworteten, dass die derzeitige Regulierung ausreichend sei. 17 % hatten keine Meinung. Nimmt man nur die Antworten von Bürgerinnen und Bürgern, so sprachen sich 55 % für ein Verbot aus.[177]

Auch gibt es eine Studie der Freien Universität Berlin und der Universität St. Gallen aus dem Jahr 2020 zur Akzeptanz von Gesichtserkennungssystemen in der Bevölkerung.[178] Im Hinblick auf die Akzeptanz von biometrischer Gesichtserkennung im öffentlichen Raum durch die deutsche Bevölkerung lieferte sie folgende Ergebnisse: 39 % waren gegen den Einsatz (davon 18 % stark dagegen, 21 % dagegen), 37 % akzeptierten die Technik (davon 8 % stark dafür, 29 % dafür), 24 % waren weder dagegen noch dafür.[179]

176 Vgl. § 100b Abs. 2 StPO.

177 Vgl. Europäische Kommission, Public Consultation on the AI White Paper Final Report, 2020, S. 11, ↗ https://digital-strategy.ec.europa.eu/en/white-paper-artificial-intelligence-public-consultation-towards-european-approach-excellence-and [19.07.2021].

178 Kostka/Steinacker/Meckel, Between Privacy and Convenience: Facial Recognition Technology in the Eyes of Citizens in China, Germany, the UK and the US, 2020, ↗ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3518857 [19.07.2021].

179 Steinacker u. a., Facial Recognition: A Cross-National Survey on Public Acceptance, Privacy, and Discrimination, 2020, S. 4, ↗ https://arxiv.org/abs/2008.07275 [19.07.2021].

Zudem gibt es auf europäischer Ebene die Bürgerinitiative „Reclaim Your Face“, die sich für ein Verbot der Technik stark macht[180], auf deutscher Ebene das Bündnis „Gesichtserkennung Stoppen“.[181]

Dies zeigt, dass die Frage der Akzeptanz noch nicht geklärt ist. Erforderlich scheint eine breite, öffentlich geführte demokratische Debatte zu sein, an der sich auch die Regierungen und Gesetzgeber beteiligen bzw. die von diesen moderiert wird. 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.[182]

Die Fragen, die sich dabei stellen, sind grundlegender Natur. In welcher Gesellschaft wollen wir leben? Wollen wir ein Mehr an Sicherheit? Sind wir dann auch bereit, im öffentlichen Raum von Gesichtserkennungssystemen überwacht zu werden?

Oder fühlen wir uns durch Gesichtserkennung zu sehr überwacht und unfrei und möchten unsere Bedürfnisse an Privatheit über ein Mehr an Sicherheit stellen? Entspricht der Einsatz von Gesichtserkennungssystemen nicht unserer Vorstellung von einem öffentlichen Raum in einer Demokratie?

Falls ja, sind wir dann aber auch bereit, die Risiken zu akzeptieren, die sich aus einem Verzicht auf die Technologie ergeben? Können wir damit leben, dass dann gegebenenfalls terroristische Anschläge nicht abgewehrt bzw. Tatverdächtige nicht verhaftet werden?

Fazit

Der deutsche Gesetzgeber dürfte wohl den Einsatz der Technologie innerhalb enger europarechtlicher und noch engerer verfassungsrechtlicher Grenzen im Rahmen des Verhältnismäßigen erlauben. Dazu müsste auch eine Überwachungs-Gesamtrechnung positiv ausfallen (doppelte Verhältnismäßigkeitsprüfung).

Der deutsche Gesetzgeber sollte die biometrische Gesichtserkennung im öffentlichen Raum allerdings wohl nur erlauben, wenn die Gesellschaft die Technologie auch will und akzeptiert. Derzeit ist die Frage der gesellschaftlichen Akzeptanz noch nicht geklärt. Es braucht eine weitergehende breite öffentliche demokratische Debatte. Bis zu deren Abschluss erscheint ein Moratorium sinnvoll.

Hierzu muss jedoch kein ausdrückliches Verbot ausgesprochen werden, da die Technik mangels Rechtsgrundlage nach dem datenschutzrechtlichen Verbot mit Erlaubnisvorbehalt derzeit bereits verboten ist. Der Gesetzgeber sollte wohl vielmehr bis zum Abschluss der demokratischen Debatte davon absehen, biometrische Gesichtserkennung im öffentlichen Raum zu erlauben, also eine Rechtsgrundlage für ihren Einsatz zu schaffen.

---

180 ↗ https://reclaimyourface.eu/de/ [19.07.2021].

181 ↗ https://gesichtserkennung-stoppen.de/ [19.07.2021].

182 Europäische Kommission (Fn. 122), S. 26.

Weitere Fälle des Einsatzes von Gesichtserkennungssystemen zur Identifikation

Einsatz von Gesichtserkennungssystemen im Zusammenhang mit dem G20-Gipfel durch die Polizei Hamburg

Ein weiterer Fall des Einsatzes von Gesichtserkennungssystemen zur Identifikation besteht im Zusammenhang mit dem G20-Gipfel durch die Polizei Hamburg. Die Polizei Hamburg hat zur Aufklärung von Straftaten anlässlich des G20-Gipfels ein Gesichtserkennungssystem 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).[183]

Der Hamburger Beauftragte für Datenschutz und Informationsfreiheit ist der Ansicht, dass bereits die Detektion (1. Schritt) und die Speicherung dieser Daten unzulässig sei, sodass auch der Abgleich (2. Schritt) nicht datenschutzgerecht sei. Es fehle bereits an einer Rechtsgrundlage für die Detektion (1. Schritt). Insbesondere komme die Ermittlungsgeneralklausel nach §§ 160, 163 StPO i. V. m. § 48 BDSG als Rechtsgrundlage nicht in Betracht. Eine allgemein gehaltene Generalklausel sei aufgrund der Schwere des Grundrechtseingriffs (Eingriff in biometrische Daten einer Vielzahl von Personen, die keinen Anlass zu der Maßnahme gegeben haben) zu unbestimmt. Eine solch wesentliche Entscheidung über eine derartige Maßnahme sollte dem Gesetzgeber vorbehalten sein, und nicht der Verwaltung, gestützt auf eine Generalklausel.

Der Hamburger Beauftragte für Datenschutz und Informationsfreiheit verweist dabei insbesondere auf die Rechtsprechung des Bundesverfassungsgerichts zur Videoüberwachung von öffentlichen Plätzen, wonach eine datenschutzrechtliche Generalklausel zur Videoüberwachung als zu unbestimmt für einen Eingriff in die Grundrechte von einer großen Anzahl von Betroffenen angesehen wurde, die durch ihr Verhalten keinen Anlass dazu gegeben haben.[184]

Die Datenschutzaufsichtsbehörde hat das Verfahren der Polizei Hamburg beanstandet und später eine Löschung der gespeicherten Daten angeordnet. Dagegen hat die Polizei Hamburg geklagt und vor dem Verwaltungsgericht Hamburg recht bekommen.[185] Insbesondere würde die Datenschutzaufsichtsbehörde nach Ansicht des Gerichts die Schwere des Eingriffs verkennen und daher unzutreffend annehmen, die Ermächtigungsnorm sei für den Eingriff zu unbestimmt. Denn es bestünden Zweifel, ob wirklich eine unbestimmte Vielzahl von Personen betroffen seien, die durch ihr Verhalten keinen Anlass zu der Maßnahme gegeben haben. Der Hamburger Beauftragte für Datenschutz und Informationsfreiheit habe nämlich nicht berücksichtigt, dass bei dem biometrischen Abgleich (2. Schritt) die Daten der Vielzahl Unverdäch-

183 VG Hamburg, Urteil vom 23.10.2019 - 17 K 203/19 - BeckRS 2019, 40195, Rn. 3 ff., beck-online.

184 Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, Datenschutzrechtliche Prüfung des Einsatzes einer Gesichtserkennungssoftware zur Aufklärung von Straftaten im Zusammenhang mit dem G20-Gipfel durch die Polizei Hamburg, S. 9 ff., ↗ https://datenschutz-hamburg.de/assets/pdf/Pruefbericht_Gesichtserkennungssoftware.pdf [19.07.2021].

185 VG Hamburg, Urteil vom 23.10.2019 - 17 K 203/19 - BeckRS 2019, 40195, beck-online.

tiger unterdrückt würden und nur diejenigen der Tatverdächtigen tatsächlich ausgeworfen werden. Auch sei der große Umfang der Datei sachlich gerechtfertigt, da beim G20-Gipfel insbesondere Straftaten aus sehr großen Versammlungen heraus begangen wurden.[186]

Der Hamburger Beauftragte für Datenschutz und Informationsfreiheit hat die Zulassung der Berufung gegen das Urteil des Verwaltungsgerichts beantragt. Der Fall ist demnach ober- bzw. höchstgerichtlich noch nicht abschließend entschieden. Das Urteil des Verwaltungsgerichts ist in der Literatur auf Kritik gestoßen.[187]

Stellungnahme

Die Ansicht des Hamburger 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 Gesichtserkennungssystemen zur Aufklärung von Straftaten im Nachgang zu Massenereignissen, die eine große Anzahl auch Unbeteiligter betrifft, sollte wohl 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 in der Strafprozessordnung normieren oder die Verwaltung sollte auf den Einsatz der Systeme verzichten.

Einsatz von Gesichtserkennungssystemen durch die Polizei des Bundes und der Länder

Ein letzter Fall des Einsatzes von Gesichtserkennungssystemen zur Identifikation ist, dass die Polizei auf Video aufgenommene Tatverdächtige mit einer Datenbank des Bundeskriminalamts abgleicht, um diese zu identifizieren. Dies geschieht beispielsweise in Bayern.

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.

---

186 VG Hamburg, Urteil vom 23.10.2019 - 17 K 203/19 - BeckRS 2019, 40195, Rn. 97 ff., beck-online.

187 Mysegades, NVwZ 2020, S. 852; Korte, ZD-Aktuell 2020, 06955; vgl. auch Wendt, ZD-Aktuell 2018, 06364, der die Rechtsauffassung des Hamburger Beauftragten für Datenschutz und Informationsfreiheit für nachvollziehbar hält.

So führt der Bayerische Landesbeauftragte für den Datenschutz aus: „Das ist eine konkrete Datenbank, die bei einem konkreten Tatverdacht durchsucht werden kann [...] das ist etwas völlig anderes als das, was in Berlin diskutiert wurde oder worum in Hamburg gestritten wird“.[188]

Gegen ein solches Verfahren bestehen keine grundsätzlichen datenschutzrechtlichen Bedenken. Es wird aufgrund eines bestehenden Tatverdachts gegen eine Person ein Abgleich mit gespeicherten Bilddateien durchgeführt. Solche Maßnahmen weisen eine geringere Eingriffsintensität als die Videoüberwachung mit biometrischer Gesichtserkennung und der Einsatz von Gesichtserkennungssystemen bei Großereignissen auf, da sie nur Personen betreffen, die einen Anlass für den Einsatz der Technik gegeben haben und keine große Streubreite haben.[189]

Rechtsgrundlage für einen solchen Abgleich dürfte § 98c StPO sein.[190] Danach dürfen zur Aufklärung einer Straftat personenbezogene Daten aus einem Strafverfahren mit anderen zur Strafverfolgung oder Strafvollstreckung gespeicherten Daten maschinell abgeglichen werden.

188 Schultejans, Bayern: Immer mehr Ermittlungserfolge dank Gesichtserkennung, in: heise online, 2020, ↗ https://www.heise.de/newsticker/meldung/Bayern-Immer-mehr-Ermittlungserfolge-dank-Gesichtserkennung-4656706.html [19.07.2021].

189 Vgl. Petri (Fn. 143), S. 148; Hornung/Schindler (Fn. 143), S. 207.

190 Hornung/Schindler (Fn. 143), S. 207.

7 Zusammenfassung und Ausblick

In der rechtswissenschaftlichen Literatur wird konstatiert: „Betrachtet man die Entwicklung der letzten Jahre, so scheint der Siegeszug der biometrischen Gesichtserkennung unaufhaltsam“.[191]

Werden Gesichtserkennungssysteme stetig mehr eingesetzt werden und welche Grenzen sollte man ihnen setzen? Bedarf es also neuer rechtlicher Vorgaben und wenn ja, welcher?

Das Entsperren von Smartphones, das Passieren einer Passkontrolle, Systeme zur Emotionserkennung[192], Clearview, PimEyes, der Test von biometrischer Gesichtserkennung im öffentlichen Raum am Bahnhof Berlin Südkreuz, der Einsatz von Gesichtserkennungssystemen beim G20-Gipfel und in der alltäglichen Polizeiarbeit: Betrachtet man die vergangenen Jahre, so ist in der Tat davon auszugehen, dass Gesichtserkennung immer mehr eingesetzt werden wird. Allerdings sollte man den Systemen klare rechtliche Vorgaben machen. Mit Ausnahme von Gesichtserkennung zum Zwecke der Authentifikation besteht rechtlicher Handlungsbedarf:

1.

Klassifizierungen mit Gesichtserkennungssystemen greifen tief in Persönlichkeitsrechte der Betroffenen ein und bergen zudem die große Gefahr von Diskriminierungen. Eine gesetzliche Rechtsgrundlage, aufgrund derer der Einsatz der Systeme zulässig wäre, ist nicht ersichtlich und kann wohl auch nicht geschaffen werden, da sie aufgrund der Schwere des Persönlichkeitseingriffs unverhältnismäßig wäre.

Gesichtserkennungssysteme dürfen daher nur auf Grundlage einer Einwilligung eingesetzt werden. In Fällen eines Machtungleichgewichts scheidet eine freiwillige Einwilligung regelmäßig aus. Somit dürfen die Systeme einwilligungsbasiert nur in eng bestimmten Fällen eingesetzt werden, insbesondere in den Bereichen Gesundheit, Wissenschaft und Sicherheit des Straßenverkehrs.

Dies ergibt sich aus einer Auslegung der bereits geltenden datenschutzrechtlichen Vorschriften. Fraglich ist, ob man – über eine Auslegung bestehender Vorschriften hinaus – die Systeme ausdrücklich gesetzlich verbieten und nur in eng bestimmten Fällen (auf Basis einer freiwilligen Einwilligung) erlauben sollte, wie es etwa der Europäische Datenschutzausschuss und der Europäische Datenschutzbeauftragte fordern.

Dies hätte freilich den Vorteil, dass die Systeme nicht allein nach Auslegung des geltenden Rechts, sondern ausdrücklich (mit Ausnahme von eng bestimmten Fällen) gesetzlich verboten sein würden.

---

191 Hornung/Schindler, DuD 2021, S. 515 (521).

192 Vgl. Stenner, Emotionale KI - Berechnete Gefühle, in: netzpolitik.org,, 2021, ↗ https://netzpolitik.org/2021/emotionale-ki-berechnete-gefuehle/ [19.07.2021].

Eine ausdrückliche gesetzliche Regelung erscheint jedoch nicht erforderlich zu sein, wenn die europäischen Datenschutzaufsichtsbehörden in einer gemeinsamen Stellungnahme das geltende Recht auslegen und die verbleibenden engen Anwendungsfälle auf Basis einer freiwilligen Einwilligung festlegen werden.

Es bleibt abzuwarten, ob die Europäische Kommission auf ein ausdrückliches gesetzliches Verbot der Systeme (mit engen Ausnahmen) „umschwenkt". Bislang hat die Europäische Kommission dazu keine Anstalten gemacht. Wenn das Europäische Parlament aber diese Linie vertreten sollte, müsste die Europäische Kommission einlenken oder der Vorschlag der Europäischen Kommission für die Regulierung von Künstlicher Intelligenz würde scheitern. Denn der Gesetzesentwurf wird im ordentlichen Gesetzgebungsverfahren nach Art. 294 des Vertrages über die Arbeitsweise der Europäischen Union beschlossen.[193] Das Europäische Parlament hat aber ebenfalls bislang keinen solchen Vorschlag gemacht.

Bleibt es also bei der geltenden datenschutzrechtlichen Rechtslage – wovon derzeit auszugehen ist –, so sollten in jedem Fall nach hier vertretener Auffassung die europäischen Datenschutzaufsichtsbehörden eine gemeinsame Stellungnahme erlassen, in der die engen Anwendungsfälle von Gesichtserkennung zum Zwecke der Klassifizierung festgelegt werden.

2.

Der Einsatz von Gesichtserkennungssystemen durch private Unternehmen wie Clearview und PimEyes zum Zwecke der Identifikation von EU-Bürgerinnen und EU-Bürgern ist verboten, da die Betroffenen regelmäßig keine Einwilligung in die Verarbeitung ihrer biometrischen Daten gegeben haben.

Es zeigt sich aber ganz deutlich ein Rechtsdurchsetzungsproblem. Auch wenn nun vier europäische Bürgerrechtsorganisationen eine Beschwerde bei den Datenschutzbehörden von Frankreich, Österreich, Italien, Griechenland und dem Vereinigten Königreich gegen Clearview eingereicht haben,[194] ist fraglich, ob die Aufsichtsbehörden von sich aus das sich datenschutzrechtlich stellende Problem von im Ausland ansässigen Unternehmen beheben können. Das zeigt auch das derzeit fruchtlose Vorgehen des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg gegen das Unternehmen PimEyes. Das Unternehmen hat schlichtweg seinen Fragenkatalog nicht beantwortet.[195]

Der Gesetzgeber ist demnach gefragt, mit den Datenschutzaufsichtsbehörden über gemeinsame Lösungen zu beraten. Gegebenenfalls bedarf es völkerrechtlicher Verträge der EU mit Drittstaaten.

---

193 Vgl. Kluth, in: Calliess/Ruffert, EUV/AEUV, 5. Auflage 2016, Art. 294 Rn. 4: „Die [...] Regelung folgt dem Grundgedanken, dass ein Rechtsakt nur bei positiver Übereinstimmung von Rat und EP erlassen werden kann."

194 Reuter (Fn. 111); Krempl (Fn. 111).

195 Kurz, PimEyes schweigt nach der Flucht auf die Seychellen, in: netzpolitik.org, 2021, ↗ https://netzpolitik.org/2021/gesichtserkennung-pimeyes-schweigt-nach-der-flucht-auf-die-seychellen/ [19.07.2021].

3.

Die biometrische Gesichtserkennung im öffentlichen Raum ist nach der hier vertretenen Auffassung in Deutschland nur unter noch engeren verfassungsrechtlichen Grenzen zulässig als den bereits engen Grenzen, die die Europäische Kommission in ihren Regulierungsvorschlägen vorsieht. Bevor eine Rechtsgrundlage auf nationaler Ebene geschaffen wird, sollte aber eine demokratische Debatte geführt werden, ob die Gesellschaft die Systeme auch will. Bis zu deren Abschluss sollte es ein Moratorium von biometrischer Gesichtserkennung im öffentlichen Raum in Deutschland geben.

Aber werden sich die Regulierungsvorschläge der EU-Kommission zu biometrischer Gesichtserkennung im öffentlichen Raum überhaupt auf EU-Ebene durchsetzen?

Hierbei ist die Meinung des Europäischen Parlaments entscheidend, da die Regulierungsvorschläge nur mit dessen Zustimmung Gesetz werden können (ordentliches Gesetzgebungsverfahren nach Art. 294 AEUV). 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.“[196]

Sollte das Europäische Parlament allerdings nicht bei seiner Haltung bleiben und die EU über kurz oder lang einen Rahmen vorgeben, innerhalb dessen der nationale Gesetzgeber die Systeme erlauben darf, so sollte der deutsche Gesetzgeber dies aber nach hier vertretener Auffassung nur innerhalb noch engerer verfassungsrechtlicher Grenzen und erst dann tun, wenn die deutsche Bevölkerung die biometrische Gesichtserkennung im öffentlichen Raum auch akzeptiert.

196 Europäisches Parlament, Entschließung vom 6. Oktober 2021 zu dem Thema: Künstliche Intelligenz im Strafrecht und ihre Verwendung durch die Polizei und Justizbehörden in Strafsachen (2020/2016(INI)), S. 15, https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_DE.pdf [19.10.2021].

4.

Über derartig Wesentliches wie den Einsatz von Gesichtserkennungssystemen zur Strafverfolgung im Nachgang zu Massenereignissen, wie den 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.

Massenereignisse wird es in Zukunft noch öfter geben. Der Gesetzgeber sollte, wenn die Systeme zukünftig wiedereingesetzt werden sollen, eine Spezialrechtsgrundlage schaffen oder die Exekutive sollte auf deren Einsatz verzichten. Die Rechtsgrundlage muss normenklar und bestimmt sein, dem Grundsatz der Verhältnismäßigkeit entsprechen und organisatorische und verfahrensrechtliche Schutzvorkehrungen aufweisen.

5.

Der Trend zum Einsatz von Gesichtserkennungssystemen zum Abgleich von auf Video aufgenommenen Tatverdächtigen mit polizeilichen Datenbanken wird sich fortsetzen. Hiergegen bestehen keine grundsätzlichen datenschutzrechtlichen Bedenken und auch kein Regulierungsbedarf.

8 Literaturverzeichnis

Apple, About Face ID Advanced Technology, 2020, ↗ https://support.apple.com/en-gb/HT208108 [19.07.2021]

Arnold, Thomas H. / Scheutz, Matthias, The "Big Red Button" Is Too Late: An Alternative Model for the Ethical Evaluation of AI Systems, in: Ethics and Information Technology 2018 (20), S. 59 ff.

Artikel-29-Datenschutzgruppe:

- Stellungnahme 02/2012 zur Gesichtserkennung bei Online- und Mobilfunkdiensten, 22.03.2012, ↗ https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp192_de.pdf [19.07.2021]
- Stellungnahme 3/2012 zu Entwicklungen im Bereich biometrischer Technologien, 27.04.2012, ↗ https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_de.pdf [19.07.2021]

Beining, Leoni, Vertrauenswürdige KI durch Standards? Herausforderungen bei der Standardisierung und Zertifizierung von Künstlicher Intelligenz, Stiftung Neue Verantwortung 2020, ↗ https://www.stiftung-nv.de/sites/default/files/herausforderungen-standardisierung-ki.pdf [19.07.2021]

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

Brink, Stefan / Wolff, Heinrich Amadeus, BeckOK Datenschutzrecht, 36. Edition, Stand: 01.05.2021, München

Bubrowski, Helene / Lohse, Eckart, Gesetzesreform: Warum hat Seehofer die Gesichtserkennung gestoppt?, in: Faz.net, 2020, ↗ https://www.faz.net/aktuell/politik/inland/gesetzesreform-warum-hat-seehofer-die-gesichtserkennung-gestoppt-16599260.html [19.07.2021]

Bundespolizeipräsidium, Abschlussbericht „Biometrische Gesichtserkennung" des Bundespolizeipräsidiums im Rahmen der Erprobung von Systemen zur intelligenten Videoanalyse durch das Bundesministerium des Innern, für Bau und Heimat, das Bundespolizeipräsidium, das Bundeskriminalamt und die Deutsche Bahn AG am Bahnhof Berlin Südkreuz, 2018, ↗ https://www.bundespolizei.de/Web DE/04Aktuelles/01Meldungen/2018/10/181011_abschlussbericht_gesichtserkennung_down.pdf [19.07.2021]

Buolamwini, Joy / Gebru, Timnit, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, in: PMLR 2018 (81), S. 77 ff., ↗ http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf [19.07.2021]

Calliess, Christian / Ruffert, Matthias, EUV/AEUV, 5. Auflage 2016, München

Chaos Computer Club, Biometrische Videoüberwachung: Der Südkreuz-Versuch war kein Erfolg, 2018, ↗ https://www.ccc.de/de/updates/2018/debakel-am-suedkreuz [19.07.2021].

Choudhury, 10 Face Datasets to Start Facial Recognition Projects, in: Analytics India Magazine, 2020, ↗ https://analyticsindiamag.com/10-face-datasets-to-start-facial-recognition-projects/ [19.07.2021]

Council of Europe:

- Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Azria, Sandra / Wickert, Frédéric), Facial Recognition: Current Situation and Challenges, 13.11.2019, ↗ https://rm.coe.int/t-pd-2019-05rev-facial-recognition-report-003-/16809eadf1 [19.07.2021]
- Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Guidelines on Facial Recognition, 28.01.2021, ↗ https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3 [19.07.2021]
- Pressemitteilung vom 28. Januar 2021, Facial Recognition: Strict Regulation Is Needed to Prevent Human Rights Violations, https://search.coe.int/directorate_of_communications/Pages/result_details.aspx?ObjectId=0900001680a12f84 [19.07.2021]

Crumpler, William, How Accurate Are Facial Recognition Systems – and Why Does It Matter?, in: CSIS - Blog, 2020, ↗ 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, Ingo / Laufer, Daniel / Meineck, Sebastian, Gesichtserkennung ist eine Waffe, in: netzpolitik.org, 2021, ↗ https://netzpolitik.org/2020/npp-204-pimeyes-gesichtserkennung-ist-eine-waffe/ [19.07.2021]

Datenethikkommission der Bundesregierung, Gutachten der Datenethikkommission der Bundesregierung, 2019, ↗ https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=6 [19.07.2021]

Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit:

- 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]
- Tätigkeitsbericht Datenschutz 2020, 2021, ↗ https://datenschutz-hamburg.de/assets/pdf/29._taetigkeitsbericht_datenschutz_2020.PDF [19.07.2021]

Deutscher Anwaltverein, Pressemitteilung PM 01/2020 vom 07.01.2020: Deutscher Anwaltverein warnt vor systematischer Videoüberwachung mit Gesichtserkennung, ↗ https://anwaltverein.de/de/newsroom/pm-01-20-dav-warnt-vor-systematischer-videoueberwachung-mit-gesichtserkennung [19.07.2021]

Ehmann, Eugen / Selmayr, Martin, Datenschutz-Grundverordnung, 2. Auflage 2018, München

Europäische Kommission:

- 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, 21.04.2021, ↗ https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0019.02/DOC_2&format=PDF [19.07.2021]
- Public Consultation on the AI White Paper – Final Report, 2020, ↗ https://digital-strategy.ec.europa.eu/en/white-paper-artificial-intelligence-public-consultation-towards-european-approach-excellence-and [19.07.2021]
- 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, 21.04.2021, ↗ https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0019.02/DOC_1&format=PDF [19.07.2021]
- Weißbuch, Zur Künstlichen Intelligenz – Ein europäisches Konzept für Exzellenz und Vertrauen, 19.02.2020, ↗ https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_de.pdf [19.07.2021]

European Data Protection Board, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, 04.05.2020, ↗ https://www.datenschutzkonferenz-online.de/media/dsgvo/Leitlinien%2005-2020%20zur%20Einwilligung%20gem%C3%A4%C3%9F%20Verordnung%202016-679.pdf [19.07.2021]

European Data Protection Board / European Data Protection Supervisor, 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), 18. Juni 2021, ↗ https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en [19.07.2021]

Europäisches Parlament, Entschließung zu dem Thema: Künstliche Intelligenz im Strafrecht und ihre Verwendung durch die Polizei und Justizbehörden in Strafsachen, 6. Oktober 2021, ↗ https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_DE.pdf [19.10.2021]

European Union Agency for Fundamental Rights, Facial Recognition Technology: Fundamental Rights Consideration in the Context of Law Enforcement, 2019, ↗ https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf [19.07.2021]

Fanta, Alexander, Künstliche Intelligenz – EU erwägt Verbot von Gesichtserkennung, in: netzpolitik.org, 2020, ↗ https://netzpolitik.org/2020/eu-erwaegt-verbot-von-gesichtserkennung/ [19.07.2021]

Floridi, Luciano u. a., AI4People – An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations, in: Minds and Machines 2018 (28), S. 689 ff.

Gola, Peter / Heckmann, Dirk, Bundesdatenschutzgesetz, 13. Auflage 2019, München

Gurovich, Yaron u. a., Identifying Facial Phenotypes of Genetic Disorders Using Deep Learning, in: Nature Medicine 2019 (25), S. 60 ff.

Held, Amélie P., Gesichtserkennung: Schlüssel oder Spitzel?, in: MMR 2019, S. 285 ff.

High-Level Expert Group on Artificial Intelligence, Policy and Investment Recommendation for Trustworthy AI, 26.06.2019, ↗ https://digital-strategy.ec.europa.eu/en/library/policy-and-investment-recommendations-trustworthy-artificial-intelligence [19.07.2021]

Hornung, Gerrit / Schindler, Stephan, Das biometrische Auge der Polizei – Rechtsfragen des Einsatzes von Videoüberwachung mit biometrischer Gesichtserkennung, in: ZD 2017, S. 203 ff.

Hornung, Gerrit / Schindler, Stephan, Datenschutz bei der biometrischen Gesichtserkennung. Künstliche Intelligenz und Musterkennung als Herausforderung für das Recht, in: DuD 2021, S. 515 ff.

Kurz, Constanze, PimEyes schweigt nach der Flucht auf die Seychellen, in: netzpolitik.org, 2021, ↗ https://netzpolitik.org/2021/gesichtserkennung-pimeyes-schweigt-nach-der-flucht-auf-die-seychellen/ [19.07.2021]

Köver, Chris, EU-Datenschutzregeln schützen nicht vor Gesichter-Suchmaschinen, in: netzpolitik.org, 2020, ↗ https://netzpolitik.org/2020/eu-datenschutzregeln-schuetzen-nicht-vor-gesichter-suchmaschinen/ [19.07.2021]

Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder:

- Entschließung: Einsatz von Videokameras zur biometrischen Gesichtserkennung birgt erhebliche Risiken, 30.03.2017, ↗ https://www.datenschutzkonferenz-online.de/media/en/20170330_en_gesichtserkennung.pdf [19.07.2021]
- Kurzpapier Nr. 5, Datenschutzfolgenabschätzung nach Art. 35 DSGVO, 17.12.2018, ↗ https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf [19.07.2021]
- Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist, 17.10.2018, ↗ https://www.lda.bayern.de/media/dsfa_muss_liste_dsk_de.pdf [19.07.2021]
- Positionspapier zur biometrischen Analyse, 03.03.2019, ↗ https://www.datenschutzkonferenz-online.de/media/oh/20190405_positionspapier-biometrie.pdf [19.07.2021]

Korte, Kai, VG Hamburg: Polizei darf Gesichtserkennungssoftware weiter einsetzen, ZD-Aktuell 2020, 06955

Kostka, Genia / Steinacker, Léa / Meckel, Miriam, Between Privacy and Convenience: Facial Recognition Technology in the Eyes of Citizens in China, Germany, the UK and the US, in: SSRN Electronic Journal, ↗ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3518857 [19.07.2021]

Krempl, Stefan, Gesichtserkennung: Europäische Bürgerrechtler gehen gegen Clearview vor, in: heise online, 2021, ↗ https://www.heise.de/news/Gesichtserkennung-Europaeische-Buergerrechtler-gehen-gegen-Clearview-vor-6055056.html [19.07.2021]

Kühling, Jürgen / Buchner, Benedikt, Datenschutz-Grundverordnung, 3. Auflage 2020, München

Kulick, Andreas, „Höchstpersönliches Merkmal" – Verfassungsrechtliche Maßstäbe der Gesichtserkennung, in: NVwZ 2020, S. 1622 ff.

Laufer, Daniel, Clearview AI verweigert Zusammenarbeit mit deutscher Datenschutzaufsicht, in: netzpolitik.org, 2020, ↗ https://netzpolitik.org/2020/gesichtserkennung-clearview-ai-verweigert-zusammenarbeit-mit-deutscher-datenschutzaufsicht/ [19.07.2021]

LTO, Neues Bundespolizeigesetz – Seehofer verzichtet auf Gesichtserkennungssoftware, 2020, ↗ https://www.lto.de/recht/nachrichten/n/entwurf-bundespolizeigesetz-kein-einsatz-software-gesichtserkennung-seehofer/ [19.07.2021]

Martinez-Martin, Nicole, What Are Important Ethical Implications of Using Facial Recognition Technology in Health Care?, in: AMA Journal of Ethics 2019 (21, 2), S. 180 ff., ↗ https://journalofethics.ama-assn.org/sites/journalofethics.ama-assn.org/files/2019-01/pfor1-1902_0.pdf [19.07.2021]

Maunz, Theodor / Dürig, Günter, Grundgesetz, Band 1, 94. Auflage 2021, München

McLaughlin, Michael / Castro, Daniel, The Critics Were Wrong: NIST Data Shows the Best Facial Recognition Algorithms Are Neither Racist Nor Sexist, ITIF 2020, ↗ https://itif.org/publications/2020/01/27/critics-were-wrong-nist-data-shows-best-facial-recognition-algorithms [19.07.2021]

Morley, Jessica u. a., From What to How: An Initial Review of Publicly Available AI Ethics Tools, Methods and Research to Translate Principles into Practices, in: Science and Engineering Ethics 2020 (26), 2141 ff., ↗ https://link.springer.com/content/pdf/10.1007/s11948-019-00165-5.pdf [19.07.2021]

Mysegades, Jan, Keine staatliche Gesichtserkennung ohne Spezial-Rechtsgrundlage, in: NVwZ 2020, S. 852 ff.

Ngan, Mei / Grother, Patrick / Hanaoka, Kayee, Ongoing Face Recognition Vendor Test (FRVT) Part 6a: Face Recognition Accuracy with Masks Using Pre-COVID-19 Algorithms, NIST, 2020, ↗ https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8311.pdf [19.07.2021]

Papier, Hans-Jürgen, Rechtsstaatlichkeit und Grundrechtsschutz in der digitalen Gesellschaft, in: NJW 2017, S. 3025 ff.

Petri, Thomas, Biometrie in der polizeilichen Ermittlungsarbeit am Beispiel der automatisierten Gesichtserkennung, in: GSZ 2018, S. 144 ff.

Poscher, Ralf / Kilchling, Michael, Pilotprojekt zur Entwicklung eines periodischen Überwachungsbarometers für Deutschland durch das Max-Planck-Institut zur Erforschung von Kriminalität, Sicherheit und Recht, Abteilung Öffentliches Recht, 2021,

↗ https://www.freiheit.org/sites/default/files/2021-03/uberwachungsbarometer_sachstandsbericht_rev_feb2021_final.pdf [19.07.2021]

Raji, Inioluwa Deborah, Saving Face: Investigating the Ethical Concerns of Facial Recognition Auditing, AIES 2020: Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society 2020, S. 145 ff.

Reuter, Markus, Datenschutz-Verfahren gegen PimEyes und Clearview, in: netzpolitik.org, 2021, ↗ https://netzpolitik.org/2021/gesichtserkennung-datenschutz-verfahren-gegen-pimeyes-und-clearview/ [19.07.2021]

Roßnagel, Alexander, Die „Überwachungs-Gesamtrechnung" – Das BVerfG und die Vorratsdatenspeicherung, in: NJW 2010, S. 1238 ff.

Schultejans, Britta, Bayern: Immer mehr Ermittlungserfolge dank Gesichtserkennung, in: heise online, ↗ https://www.heise.de/newsticker/meldung/Bayern-Immer-mehr-Ermittlungserfolge-dank-Gesichtserkennung-4656706.html [19.07.2021]

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

Steinacker, Léa u. a., Facial Recognition: A Cross-National Survey on Public Acceptance, Privacy and Discrimination, ICML 2020: Proceedings of the 37th International Conference on Machine Learning Law and ML Workshop, ↗ https://arxiv.org/abs/2008.07275 [19.07.2021]

Stenner, Pia, Emotionale KI – Berechnete Gefühle, in: netzpolitik.org, 2021, ↗ https://netzpolitik.org/2021/emotionale-ki-berechnete-gefuehle/ [19.07.2021]

The Medical Futurist, Your Guide to Facial Recognition Technology in Healthcare, 2019, ↗ https://medicalfuturist.com/your-guide-to-facial-recognition-technology-in-healthcare/ [19.07.2021].

Thiel, Markus, Die Vermessung der Welt? – Zur Nutzung biometrischer Identifikationssysteme durch die Sicherheitsbehörden, in: ZPR 2016, S. 218 ff.

Wendt, Kai, Rechtsgrundlage zur automatisierten Gesichtserkennung in Strafverfahren, ZD-Aktuell 2018, 06364

Wissenschaftlicher Dienst des Bundestages, Sachstand – Rechtsgrundlage für den Einsatz sog. intelligenter Videoüberwachung durch die Bundespolizei, 2016, ↗ https://www.bundestag.de/resource/blob/439670/e2efe42f49749393cc701c7c4f9af7d8/wd-3-202-16-pdf-data.pdf [19.07.2021]

ZDFheute, Gesichtsdatenbank „PimEyes" – „Hochgefährliche" Suchmaschine, 2020, ↗ https://www.zdf.de/nachrichten/digitales/pimeyes-gesichtserkennung-100.html [19.07.2021]

9 Rechtsprechungsverzeichnis

BVerfG NJW 1984, 419, Urteil vom 15.12.1983 - 1 BvR 209/83 u. a. – Volkszählungsurteil

BVerfG NJW 2006, 1939, Beschluß vom 04.04.2006 - 1 BvR 518/02 – Rasterfahndung

BVerfG NVwZ 2007, 688, Beschluß vom 23.02.2007 - 1 BvR 2368/06 – Videoüberwachung an öffentlichen Plätzen

BVerfG NJW 2008, 822, Urteil vom 27.02.2008 - 1 BvR 370/07, 1 BvR 595/07 – Online-Durchsuchung

BVerfG MMR 2008, 308, Urteil vom 11.03.2008 - 1 BvR 2074/05 und 1 BvR 1254/07 – Kennzeichen I

BVerfG MMR 2010, 356, Urteil vom 02.03.2010 - 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 – Vorratsdatenspeicherung

BVerfG NJW 2019, 827, Beschluss vom 18.12.2018 - 1 BvR 142/15 – Kennzeichen II

VG Hamburg, Urteil vom 23.10.2019 - 17 K 203/19 – BeckRS 2019, 40195, beck-online

www.bidt.digital

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