Neue Zeitschrift für Verwaltungsrecht – Extra

In Zusammenarbeit mit der Neuen Juristischen Wochenschrift

Gegründet von Rechtsanwalt **Prof. Dr. Hermann Weber**, Schriftleiter von 1982–2001

Herausgegeben von **Prof. Dr. Martin Burgi,** München – **Prof. Dr. Christian Calliess,** Berlin – **Dr. Josef Christ,** Richter des BVerfG, Karlsruhe – **Prof. Dr. Klaus-Peter Dolde,** Rechtsanwalt, Stuttgart – **Dr. Frank Fellenberg,** Rechtsanwalt, Berlin – **Prof. Dr. Andreas Heusch,** Präsident des VG, Düsseldorf – **Prof. Dr. Thomas Mayen,** Rechtsanwalt, Bonn – **Prof. Dr. Hubert Meyer,** Geschäftsf. Vorstandsmitglied des Niedersächsischen Landkreistages, Hannover – **Prof. Dr. Janbernd Oebbecke,** Münster – **Prof. Dr. Joachim Scherer,** Rechtsanwalt, LL.M., Frankfurt a. M. – **Dr. Heribert Schmitz,** Ministerialrat a. D., Berlin – **Prof. Dr. Friedrich Schoch,** Freiburg – **Dr. Thomas Schröer,** Rechtsanwalt, Frankfurt a. M. – **Prof. Dr. Rudolf Streinz,** München

Schriftleitung: Rechtsanwalt **Prof. Dr. Achim Schunder** und Rechtsanwältin **Dr. Christiane Prause,** Beethovenstraße 7 b, 60325 Frankfurt a. M.

1-2 2022

Seite 1–16
41. Jahrgang
15. Januar 2022

Professor Dr. Mario Martini*

Gesichtserkennung im Spannungsfeld zwischen Sicherheit und Freiheit

Rund eine Milliarde Videoüberwachungskameras sind rund um den Globus installiert. Immer häufiger kommen dabei auch Gesichtserkennungssysteme zum Einsatz. Für diese ist es längst kein technischer Herkulesakt mehr, eine Person allein auf der Grundlage einer beliebigen Fotoaufnahme an jedem denkbaren Ort zu identifizieren. Welchen rechtlichen Rahmenbedingungen der präventive Einsatz automatisierter Gesichtserkennung in der Polizeiarbeit unterworfen ist, analysiert der Beitrag am Beispiel dreier praktisch relevanter Einsatzszenarien.

* Der Autor ist Inhaber des Lehrstuhls für Verwaltungswissenschaft, Staatsrecht, Verwaltungsrecht und Europarecht der Universität Speyer sowie Leiter des Programmbereichs „Digitalisierung“ am Forschungsinstitut für öffentliche Verwaltung.

Er dankt den Forschungsreferent(inn)en Lukas von Brasch, Carolin Kemper, Martin Feldhaus, Michael Kolain, Luise Warmuth und Christine Sophie Wiesehöfer für die inhaltliche Mitwirkung.

Soweit nicht anders vermerkt, datieren Internetquellen vom 30. September 2021.

I. Gesichtserkennung auf dem Weg in den Alltag der Menschen

Gesichtserkennung ist eine der sensibelsten Spielarten Künstlicher Intelligenz. Verschwand der Einzelne früher bei Überblicksaufnahmen einer Überwachungskamera gleichsam gesichtslos in der Masse, kann eine biometrische Analyse die Polizei heute in Sekundenschnelle zum Täter führen.

Welche Sprengkraft die Technologie birgt, rückte Anfang 2020 in den Fokus weltweiter Aufmerksamkeit. Zu dieser Zeit drang ans Licht der Öffentlichkeit, dass die Firma *Clearview AI* biometrische Daten aus drei Milliarden öffentlich zugänglichen Fotos sozialer Netzwerke – unter anderem von *Facebook*,[1] *Twitter* oder *Instagram* – (ohne Einverständnis der Betroffenen) in seine Datenbank eingespeist hat. Mehr als 600 Sicherheitsbehörden rund um den Globus – vor allem in den USA,[2] aber auch in Belgien, Frankreich und den Niederlanden[3] – nutzten oder testeten die Software im Jahr 2020 bereits.[4] Insbesondere in Fällen des Kindesmissbrauchs hat sie spektakuläre Ermittlungserfolge erzielt.

Ihr dystopisches Potenzial ist jedoch ebenso mit Händen zu greifen: Nicht nur zum Stalking lässt sich die Software missbrauchen. Sie liefert auch ein polizeiliches Werkzeug, um bspw. sämtliche Teilnehmer einer Veranstaltung lückenlos zu identifizieren. *Clearview* begeht damit einen Tabubruch: Das Unternehmen verankert Gesichtserkennung als ubiquitär einsetzbares, zustimmungsfreies Identifizierungsinstrument in der freiheitlichen Gesellschaft und hebt dadurch die Anonymität des Alltäglichen faktisch auf.[5] Wer ein Bild im Internet hochlädt, rechnet eben nicht damit, dass er dadurch überall auf der Welt verfolgbar wird.

Auch die öffentlich einsehbare (biometrische) Bilddatenbank *Pim-Eyes* brachte Gesichtserkennungssysteme vielerorts in die Schlagzeilen. Die Software ermöglicht es, Fotos hochzuladen, um das Gesicht mit millionenfach gespeicherten biometrischen Daten abzugleichen.[6] Die Suche nach fremden Gesichtern wird damit zu einem Kinderspiel.

1. Internationale Entwicklungen

Auch jenseits von Clearview und Pim-Eyes dringt Gesichtserkennungstechnologie in vielen Teilen der Welt immer stärker in das Leben der Menschen vor. So sind an zahlreichen internationalen Flughäfen „E-Gates“ Routine. Dort können Reisende auf freiwilliger Basis spezielle Tore nutzen, um mithilfe des biometrischen Reisepasses einen schnellen Identitätsabgleich zu ermöglichen. In autokratischen Staaten wie China sind sog. *Smart Cams* längst als Identifizierungsinstrument im Alltag der Menschen angekommen.[7] Sie ermöglichen nicht nur den Abhebevorgang am Bankautomaten,[8] sondern auch den Zugang zum Büro oder zu öffentlichen Einrichtungen wie dem Zoo.[9] In Moskau können die Fahrgäste der U-Bahn ihre Fahrkarten unterdessen via Facepay bezahlen.[10] Gesichtserkennungstechnologie dient der russischen Regierung nicht zuletzt als Überwachungsmittel, um Regimekritiker engmaschig zu beobachten: Mit ihrer Hilfe identifiziert sie Oppositionelle, wie bspw. die Unterstützer *Nawalnys*, die an Veranstaltungen teilnehmen.[11]

In vielen westlichen Staaten formieren sich Proteste gegen den Vormarsch der Gesichtserkennungstechnologie; Aktivisten schminken sich gezielt und tragen Masken, um der KI-gestützten Mustererkennung zu entkommen.[12] Das wachsende Unbehagen hat das soziale Netzwerk Facebook unterdessen dazu veranlasst, die Gesichtserkennungsfunktion seines Dienstes einzustellen.[13] Einzelne Bundesstaaten der USA schränken den staatlichen Einsatz von *Smart Cams* bis auf Weiteres regulatorisch ein oder untersagen ihn vollständig. Die Stadt San Francisco[14] sowie der gesamte US-Staat Kalifornien[15] haben bereits Moratorien erlassen. In Illinois bindet der *Biometric Information Privacy Act* aus dem Jahr 2008 es an die Zustimmung des Betroffenen, individuelle Merkmale des Gesichts auszuwerten.[16] Ähnliches gilt in Texas.[17]

2. Entwicklungen in Europa

Für die *Europäische Union* hatte die Kommission noch Ende 2019 ein Moratorium für staatliche Gesichtserkennung –

1 In der Vergangenheit trainierte Facebook seine Gesichtserkennungssoftware, indem es seinen Nutzern vorschlug, in Fotos Freunde mit deren Namen zu markieren. Da Facebook dafür keine Einwilligung eingeholt hatte, musste das Unternehmen Entschädigungen in Höhe von insgesamt 650 Millionen US-Dollar zahlen, vgl. Facebook zahlt 650 Millionen Dollar in US-Verfahren zu Gesichtserkennung, beck-aktuell vom 1.3.2021.
2 Hill, The Secretive Company That Might End Privacy as We Know It, The New York Times online vom 18.1.2020.
3 Wölbert/Krempl, Nicht nur in China und den USA, auch in der EU setzen Fahnder auf Gesichtserkennungssoftware – und auf das umstrittene Clearview-System, heise online vom 17.3.2020.
4 Hill (Fn. 2); das heißt nicht, dass Menschen in Deutschland nicht von Clearview AI betroffen sein können, vgl. Montag/Mcleod et al., The Rise and Rise of Biometric Mass Surveillance in the EU, 2021, S. 25 ff.
5 Das Geschäftsmodell des Unternehmens wirft viele Fragen auf. In den USA sind zahlreiche Sammelklagen anhängig. Im Zentrum steht die Frage, ob es unzulässig ist, öffentlich zugängliche Bilder zu kopieren (sog. Scraping), oder ob dies von der Meinungsfreiheit des ersten Zusatzartikels der amerikanischen Verfassung gedeckt ist.
6 Vgl. Laufer/Meineck, Eine polnische Firma schafft gerade unsere Anonymität ab, netzpolitik.org vom 10.7.2020.
7 Siehe zu dieser Entwicklung bspw. Denyer, Beijing bets on facial recognition in a big drive for total surveillance, The Washington Post online vom 7.1.2018.
8 Vgl. Ankenbrand, China hat das wertvollste KI-Startup der Welt, faz.net vom 9.4.2018
9 Siehe zur Klage eines chinesischen Jura-Professors gegen Gesichtserkennung bspw. Böge, Was darf ein Zoo?, faz.net vom 6.11.2019.
10 dpa, Mit dem Gesicht bezahlen, FAZ vom 19.10.2021, S. 25.
11 Klimeniouk, Der digitale Gulag, FAZ vom 16.5.2021, S. 43.
12 Dana, Portraits of Hong Kong's masked protesters – in pictures, The Guardian online vom 13.11.2019; JaSartorius, 36C3: Schminke führt Gesichtserkennung in die Irre, heise.de vom 28.12.2019. So entwickelt sich sogar eine eigene Kunstform der Fotografie, die mit den Mitteln der Malerei und der Mode Gesichter so zu verändern versucht, dass Gesichtserkennungsprogramme an ihnen scheitern. Vgl. dazu Maak, Schön unsichtbar, FAS vom 31.10.2021, S. 33.
13 lid., Facebook will künftig auf Gesichtserkennung verzichten, FAZ vom 4.11.2021, S. 26.
14 Congar/Fausset et al., San Francisco Bans Facial Recognition Technology, The New York Times online vom 14.5.2019.
15 Für die Nutzung im Zusammenhang mit Body Cams: Thebault, California could become the largest state to ban facial recognition in body cameras, The Washington Post online vom 12.9.2019.
16 Illinois Biometric Information Privacy Act (740 ILCS 14) von 2008. Eine kurze Übersicht der Regelungen findet sich unter https://www.aclu-il.org/en/campaigns/biometric-information-privacy-act-bipa.
17 Tex. Bus. & Com. Code § 503.001 (Capture or Use of Biometric Indentifier Act) stellt die Verarbeitung biometrischer Kennzeichen, wie Fingerabdrücke, Iris-Scans oder Stimmerkennung, unter bußgeldbewehrten Einwilligungsvorbehalt. Im Unterschied zum BIPA gibt es kein privates Klagerecht. Mittlerweile hat der Bundesstaat Washington eine ähnliche Regelung erlassen (Wash. Rev. Code Ann. § 19.375.020).

zunächst begrenzt auf fünf Jahre – erwogen.[18] Davon ist sie jedoch in ihrem Weißbuch zur Künstlichen Intelligenz vom Februar 2020[19] abgerückt. Der Vorschlag für ein Gesetz über Künstliche Intelligenz 2021[20] will Gesichtserkennung in öffentlichen Räumen unter engen materiellen und verfahrensrechtlichen Voraussetzungen zulassen (Art. 5 I lit. d, II–IV des Entwurfs).[21] Die Kommission ist derweil im Begriff, mit verschiedenen Partnern Assistenzsysteme für Polizeibehörden zu entwickeln, um Bildmaterial aus sozialen Medien und Co. mithilfe von Gesichtserkennungstechnologie auf einer gemeinsamen Plattform biometrisch auswerten zu können.[22] Ebenso will die Union die Weichen dafür stellen, einen unkomplizierten Austausch biometrischer Bilddatenbanken zwischen den Mitgliedstaaten zu ermöglichen. Zu diesem Zweck steht die Überlegung im Raum, den sog. Prümer Vertrag über die Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus, der grenzüberschreitenden Kriminalität und der illegalen Migration,[23] zu erweitern.[24]

In den einzelnen *europäischen Nationalstaaten* hat Gesichtserkennung zwar noch keine weite Verbreitung gefunden. Auch dort ist sie aber auf dem Vormarsch. So beschloss die französische Regierung im Jahr 2019 (neben der umstrittenen Nutzung von *Clearview AI*[25]), das elektronische Identifikationssystem „Alicem" einzuführen, das automatisierte Gesichtserkennung nutzt.[26] Als Zugangskontrolle für Schulen sollte sie ebenfalls zum Einsatz kommen. Die französische Datenschutzbehörde stufte das jedoch als unzulässig ein.[27] Im Vereinigten Königreich ist Gesichtserkennung demgegenüber bereits im schulischen Alltag angekommen: An der Westküste Schottlands konnten Schüler an einigen Schulen des Bezirks North Ayrshire ihr Essen kontaktlos via Gesichtserkennung bezahlen.[28] Proteste von Datenschützern setzten dieser Praxis jedoch ebenso vorläufig ein Ende. In London ist Gesichtserkennung weiter vorgedrungen: Dort unterstützt sie die Polizeibeamten bei der Suche nach Straftätern.[29] Trotz heftiger Kritik hält die Londoner Polizei daran fest.[30]

In *Deutschland* erschien es lange allenfalls als eine dystopische Zukunftsvision, Spielarten einer intelligenten Videoüberwachung, insbesondere Gesichtserkennungssoftware, einzusetzen. Ihre technischen Möglichkeiten wecken jedoch zunehmend auch hierzulande Begehrlichkeiten der Sicherheitsbehörden. Von August 2017 bis Februar 2018 testete bspw. die Bundespolizei intelligente Videotechnik zur Gesichtserkennung im Bahnhof Berlin Südkreuz.[31] In markierten Bereichen erfasste das System biometrische Daten der Gesichter einzelner Fahrgäste und glich diese mit Lichtbildern von Testpersonen in einer Datenbank ab. Die Bewertung der Testphase fällt unterschiedlich aus. Während die Bundespolizei sie als Erfolg einstuft,[32] sieht der Chaos Computer Club das Projekt in einem dunklen Licht.[33]

Bei diesem eng umgrenzten Testszenario blieb es nicht. Die Hamburger Strafverfolgungsbehörden nutzten im Kontext des G20-Gipfels die Gesichtserkennungssoftware „Videmo 360",[34] um Straftäter zu identifizieren, die an den gewaltsamen Ausschreitungen in der Hansestadt beteiligt waren. Sie entfachten damit eine rege öffentliche Diskussion.[35]

Auf Bundesebene steht das rechtliche Schicksal der Gesichtserkennungssoftware als staatliches Instrument der Gefahrenabwehr gegenwärtig noch in den Sternen.[36] Im Jahr 2019 hatte ein Referentenentwurf des BMI noch umfangreiche neue Kompetenzen der Bundespolizei für den Einsatz von Gesichtserkennungssoftware an Flughäfen und Bahnhöfen vorgesehen.[37] Eine spätere Fassung aus dem Januar 2020 kannte diesen Passus indes nicht mehr.[38] Die Ampel-Koalition distanziert sich in ihrem Koalitionsvertrag von Gesichts-

18 Europäische Kommission, Structure for the White Paper on artificial intelligence – a European approach, 12.12.2019, S. 15; vgl. auch Fanta, EU erwägt Verbot von Gesichtserkennung, netzpolitik.org vom 17.1.2020.

19 Dabei handelt es sich um ein Strategiekonzept der Europäischen Kommission für Daten und Künstliche Intelligenz vom 19.2.2020, Com (2020) 65 final.

20 Vorschlag für ein Gesetz über Künstliche Intelligenz vom 22.4.2021, COM(2021) 206 final.

21 Demgegenüber sprachen sich der Europäische Datenschutzbeauftragte und der Europäische Datenschutzausschuss in einer Gemeinsamen Stellungnahme gegen den Einsatz automatisierter Gesichtserkennung im öffentlichen Raum aus, European Data Protection Board (EDPB), KI zur automatisierten Erkennung menschlicher Merkmale und andere KI-Nutzungen mit Diskriminierungsrisiko: EDSA und EDSB rufen zu Verbot auf, Pressemitteilung v. 21.6.2021. Die Vorsitzenden des EDPB, Andrea Jelinek und Wojciech Wiewiórowski, mahnen: „Die Verwendung von biometrischen Fernidentifikationssystemen im öffentlichen Raum bedeutet das Aus für die Anonymität" (aaO). Auch der Innenausschuss des EU-Parlaments forderte mit Blick auf das Risiko einer Massenüberwachung ein Moratorium, Europäisches Parlament, Artificial Intelligence in policing: safeguards needed against mass surveillance, Pressemitteilung v. 29.6.2021; siehe auch Fanta, Biometrische Überwachung: EU-Abgeordnete fordern Auszeit für Gesichtserkennung, netzpolitik.org vom 30.6.2021. Dazu auch im Einzelnen V. 4.

22 Monroy, EU entwickelt Abhörplattform mit Sprachanalyse und Gesichtserkennung, netzpolitik.org vom 12.10.2020.

23 Den Prümer Vertrag (Vertrag über die Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus, der grenzüberschreitenden Kriminalität und der illegalen Migration; abgeschlossen am 27.5.2005) haben 13 EU-Mitgliedstaaten unterzeichnet. Er soll die grenzüberschreitende Verfolgung und Bekämpfung des Terrorismus bzw. der grenzüberschreitenden Kriminalität verbessern. Er trifft auch Vorgaben, die die Übermittlung von Daten und Informationen sowie den Abgleich von DNA- oder Fingerabdruckregistern betreffen.

24 Betroffen ist Art. 9 des Prümer Vertrags zum automatisierten Abruf von daktyloskopischen Daten. Siehe dazu BT-Drs. 19/9407, S. 1; Ratsdokument 13426/18.

25 Mac/Haskins et al., Clearview´s Facial Recognition App has been used by the Justice Department, ICE, Macy´s, Walmart, and the NBA, BuzzFeed News vom 27.2.2020.

26 Über dieses System sollen die Bürger auf rund 500 Dienste der französischen Verwaltung zugreifen können. Hierzu zählt bspw. die Option, einen neuen Reisepass zu beantragen oder den Wohnsitz umzumelden. Vgl. Kormann, Frankreich will Gesichtserkennung einführen – weshalb sich das Land vor einer totalen Überwachung fürchtet, NZZ online vom 26.11.2019.

27 Commission Nationale de l´Informatique et des Libertés (CNIL), Facial recognition: for a debate living up to the challenges, 19.12.2019.

28 Maron, Britische Schulen: Schon wieder Schluss mit Gesichtserkennung, Inside-IT.ch vom 26.10.2021.

29 Haeflinger, Londoner Polizei setzt Kameras zur Gesichtserkennung ein, NZZ online vom 26.1.2020.

30 Wittenhorst, Gesichtserkennung in London: Schlechte Trefferrate und wohl ohne Rechtsgrundlage, heise.de vom 6.7.2019.

31 Bundespolizei, Test zur Gesichtserkennung am Bahnhof Berlin Südkreuz gestartet, 10.8.2017. Zu einem Testverfahren am Mainzer Hauptbahnhof siehe Schindler, Biometrische Videoüberwachung, 2020, S. 193 ff.

32 Bundespolizei, Abschlussbericht des Teilprojekts 1 "Biometrische Gesichtserkennung", 18.9.2018, S. 8: „Mehrwert", S. 20: „geeignet".

33 Chaos Computer Club, Biometrische Videoüberwachung: Der Südkreuz-Versuch war kein Erfolg, 13.10.2018.

34 Die Software wandelt menschliche Gesichter in Kodierungen um, indem sie diese biometrisch auswertet und die Datensätze in einer Referenzdatenbank speichert, und gleicht Templates Verdächtiger mit der Datenbank ab.

35 Siehe zur Kritik Monroy, Kritik an G20-Gesichtserkennung: "Neue Dimension staatlicher Ermittlungs- und Kontrolloptionen", netzpolitik.org vom 31.8.2018; über den Einsatz der Software hat das VG Hamburg mit Urt. v. 23.10.2019 entschieden, vgl. VG Hamburg, 23.10.2019 – 17 K 203/19, BeckRS 2019, 40195.

36 Zum Einsatz automatisierter Gesichtserkennung in Deutschland, vgl. Montag/Mcleod et al. (Fn. 5), S. 19 ff.

37 Dahlkamp/Knobbe et al., Seehofer will Gesichtserkennung an Bahnhöfen und Flughäfen einführen, Spiegel Online vom 3.1.2020.

38 Laufer, Innenministerium streicht automatisierte Gesichtserkennung, netzpolitik.org vom 24.1.2020.

erkennung als Instrument, um den öffentlichen Raum zu überwachen.[39]

Der Freistaat Sachsen ist demgegenüber einen Schritt weiter gegangen. Er hat die präveniv-polizeiliche Gesichtserkennung derweil erstmalig gesetzlich verankert: Sein Polizeivollzugsdienstgesetz legitimiert die Polizei dazu, Gesichtserkennungssoftware im Grenzgebiet zu Polen und Tschechien einzusetzen (§ 59 SächsPVDG).[40]

II. Technische Grundlagen

1. Funktionsweise

Während konventionelle Videotechnik sich darauf beschränkt, Bilder und Ton aufzunehmen bzw. aufzuzeichnen, damit Polizeibeamte die Daten anschließend manuell auswerten, automatisieren sog. *Smart Cams* die Analyse und heben Videoüberwachung[41] damit auf eine neue Stufe der Optimierung:[42] Sie übermitteln das Bildmaterial an ein Computersystem, das binnen eines Wimpernschlags große Silos biometrischer Daten zu durchstöbern vermag. Die Anwendungen können Live-Bilder mit externen Datenquellen, wie (Fahndungs-)Datenbanken gesuchter Personen, abgleichen oder auffällige Verhaltensweisen erkennen und automatisch Maßnahmen einleiten, etwa unverzüglich Einsatzkräfte alarmieren. Ein lernfähiges System perfektioniert damit die Verarbeitungsleistung und macht identifizierbar, was dem menschlichen Betrachter mitunter entgangen wäre.[43]

Gesichtserkennung ist nicht nur als *Echtzeitsystem* denkbar, das den Abgleich mit der Referenzdatenbank ohne substanzielle zeitliche Verzögerung vornimmt. Sie kann auch *asynchron* erfolgen. Das System gleicht dann gespeicherte Bilder eines polizeilich beobachteten Geschehens, z. B. einer potenziellen Straftat, ex post mit einer Datenbank von Bildern ab.

In beiden Fällen macht sich Gesichtserkennung eine wichtige Eigenschaft des Gesichts zunutze: Biometrische Merkmale sind nur schwer veränderbar und eignen sich damit in besonderer Weise, um eine Person zweifelsfrei zu identifizieren. Die Software greift dabei vor allem auf solche Gesichtsmerkmale zurück, die von der gegenwärtigen Mimik entkoppelt sind, also insbesondere Kanten der Augenhöhlen, die Areale um die Wangenknochen und die Seitenpartien des Mundes.[44] Merkmale wie die Iris und den Abstand zwischen Augen und Nase vergleicht das daraus abgeleitete Template dann mit den Parametern gespeicherter Gesichtsbilder oder anderer Datenbankaufnahmen. Auswertungsziele sind die *positive Identifikation* (z. B. durch Abgleich mit vorhandenen Passfotos), der *Nicht-Trefferfall* oder die *untersuchende Identifikation* (z. B. durch Abgleich des Tatortfotos mit anderen der Polizei zur Verfügung stehenden Daten).[45]

Die technische Kompetenz des Systems erschöpft sich längst nicht darin, gesuchte Personen zu *erkennen*. Seine Funktionen ermöglichen es auch, die Bilddaten mehrerer Kameras in einer zentralen Datenbank *zusammenzuführen*, um z. B. anhand der aufgezeichneten Bilder Bewegungsprofile einzelner Personen anzufertigen oder zu erfassen, ob eine Person einen bestimmten Ort regelmäßig aufsucht. Gesichtserkennung eignet sich daher im Grundsatz auch, um Personen zu beobachten, ihr Verhalten auszuwerten und darauf aufbauend Gefahren abzuwehren und effektive Strafverfolgung zu betreiben.

2. Alternative Technologien intelligenter Videoüberwachung

Intelligente Videoüberwachung kann nicht nur biometrische Merkmale des Gesichts auswerten, sondern auch auffällige Gegenstände (a) erkennen und Verhaltensmuster (b) entschlüsseln.

a) Gegenstandserkennungssoftware

Gegenstandserkennungssoftware ist in der Lage, herrenlose Gepäckstücke oder sonstige gefahrträchtige Objekte zu registrieren und im Trefferfall Sicherheitskräfte zu alarmieren.[46] Wie lange ein erfasster Gegenstand unbewegt bleiben darf, bevor das System die Alarmmeldung auslöst, ist flexibel und umgebungsspezifisch programmierbar.[47] Dadurch lassen sich im Idealfall bspw. Kofferbomben an belebten Orten rechtzeitig ausfindig machen und entschärfen.

b) Verhaltensmustererkennung

Sind Systeme auf Verhaltensmuster ausgerichtet, erkennen sie auffälliges Auftreten oder Bewegungsmuster, wie die Schrittgeschwindigkeit von Personen und Objekten sowie ihren Zustand (Person ist aufgeregt oder hilfsbedürftig) – oder auch kontextbasierte Standardereignisse und -szenarien, etwa Ansammlungen von Personenmengen.[48] Dafür rekurriert die Software auf ein Modell menschlichen Verhaltens, das entweder einen erwünschten Zustand (Whitelist-Ansatz) oder unerwünschte, gefährliche Verhaltensweisen (Blacklist-Ansatz) klassifiziert.

Beim *Whitelist-Ansatz* überprüft das System die Bilddaten, welche die Kamera aufnimmt, darauf, ob sie vom modellierten Verhalten *abweichen*. Sind also bestimmte Verhaltensweisen (wie normales Gehen oder Stehen) als Normalverhalten definiert, meldet das System andere Handlungen, wie Rennen oder Liegen, als deviant. Dieser technischen Grundlogik folgend installierte etwa die Stadt Mannheim an kriminalitätsgefährdeten Orten Software, die auffällige Bewegungen wie Treten, Schlagen und Fallen registriert sowie zwischen Menschen und Gegenständen unterscheidet.[49]

Systeme, die nach dem *Blacklist-Ansatz* operieren, prüfen das Bildmaterial hingegen darauf, ob es mit den modellierten gefährlichen Verhaltensweisen (etwa Gewaltanwendung oder dauerhaftes Aufhalten an einem Ort) *übereinstimmt*.[50]

39 SPD/Grüne/FDP, Mehr Fortschritt wagen, S. 109.
40 Siehe dazu im Einzelnen unten IV. 2.
41 Zu weiteren Terminologien im Zusammenhang mit dieser Technologie (bspw. „Automated Surveillance“ oder „Algorithmic Surveillance“), siehe Kees, Algorithmisches Panopticon, 2015, S. 38 f.
42 Bretthauer, Intelligente Videoüberwachung, 2017, 35 ff. m. w. N.; Held, Intelligente Videoüberwachung, 2014, 21 m. w. N.; Kees, Algorithmisches Panopticon, 17 f.; vgl. auch Desoi, Intelligente Videoüberwachung, 2017, 25 f. m. w. N.
43 Bretthauer, Intelligente Videoüberwachung S. 35 ff.; Held, Intelligente Videoüberwachung S. 21; Kees, Algorithmisches Panopticon S. 17 f.
44 Bundesamt für Sicherheit in der Informationstechnik (BSI), Biometrie – Gesichtserkennung, https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Technologien_sicher_gestalten/Biometrie/BiometrischeVerfahren/Gesichtserkennung/gesichtserkennung_node.html.
45 Vgl. dazu Grother/Ngan et al., Ongoing Face Recognition Vendor Test (FRVT), November 2018, S. 4.
46 Siehe dazu die Eingriffsgrundlage des § 44 Abs. 4 bwPolG; zur Presseberichterstattung siehe bspw. Biselli, „Projekt Sicherheitsbahnhof“: Intelligente Videoüberwachung am Berliner Südkreuz startet im Herbst, netzpolitik.org vom 12.4.2017; Startschuss für die algorithmenbasierte Videoüberwachung beim Polizeipräsidium Mannheim, Pressemitteilung v. 3.12.2018.
47 GIT Sicherheit, Automatisierte Bildauswertung macht die Videoüberwachung intelligent (2.11.2021), https://www.git-sicherheit.de/produkte/automatisierte-bildauswertung-macht-die-videoueberwachung-intelligent.
48 Siehe dazu Art. 33 V BayPAG; vgl. auch Bretthauer, Intelligente Videoüberwachung S. 40 ff. m. w. N.; Kees, Algorithmisches Panopticon, S. 44.
49 Andere Städte erwägen, diesem Beispiel zu folgen. Vgl. dpa, Polizei: Smarte Videoüberwachung hilft, Süddeutsche Zeitung vom 24.8.2020.
50 Kees, Algorithmisches Panopticon, S. 43.

In beiden Fällen ist die Software nicht auf die persönlichkeitsrechtlich sensible Funktionalität angewiesen, das Gesicht oder andere biometrische Merkmale zu analysieren.[51]

Noch weiter am Horizont scheint die Analyse der Gangart als Methode sicherheitstechnischer Identifizierung auf. Künstliche Intelligenz ermittelt dann auf der Grundlage von Videoaufnahmen und eines Abgleichs mit den erlernten individuellen Verhaltensweisen die Identität einzelner Personen.

3. Technische Leistungsfähigkeit und ihre Grenzen

Wie verlässlich die derzeit verfügbaren Smart-Cam-Systeme sind, darüber gehen die Meinungen auseinander. Bisherige Untersuchungen attestieren der Software zwar beachtliche Entwicklungsfortschritte – vor allem, weil sie auf neuere Methoden der *Deep Neural Networks*[52] zurückgreift:[53] Je mehr Datenmaterial die Software inspiziert, desto besser wird sie. KI-Software kann dadurch in immer schnellerem Takt unzählige Fotos analysieren und lernen, zuverlässige Vorhersagen darüber zu treffen, welche Bilder von derselben Person stammen oder welchem Gegenstand sie zuzuordnen sind.

Gleichwohl haftet den Anwendungen immer noch eine erhebliche Fehlerquote[54] an.[55] Insbesondere bei Personen mit dunkler Hautfarbe täuschen sich die Systeme noch sehr häufig; bei dunkelhäutigen Frauen beträgt die Gesamtfehlerquote bis zu 34 % (im Verhältnis zu 0,8 % für hellhäutige Männer).[56] Dies gründet vor allem auf Trainingsfehler, namentlich nicht repräsentative oder unvollständige Datenbanken:[57] Ist ein Geschlecht oder eine Ethnie in der Datenbasis über- oder unterrepräsentiert, verfälscht das die Neutralität des Outputs.[58] Gerade in jüngerer Zeit häufen sich Berichte über unrechtmäßige Verurteilungen dunkelhäutiger Personen, die auf Fehler der Gesichtserkennungssoftware zurückgehen.[59]

Während sich ein *Unternehmen* mit Fehlerquoten von bis zu einem Drittel durchaus arrangieren kann, wenn es Gesichter auswertet, um seine Marketingaktivitäten zu optimieren, sind solche Größenordnungen bei *staatlichen Eingriffsmaßnahmen* mit Blick auf ihre potenziell gewichtigen Folgen nicht tolerierbar.

III. Allgemeine unionsrechtliche und grundrechtliche Vorgaben

Setzt die Polizei Gesichtserkennungstechnologie ein, übt sie zwar originäre (national-)staatliche Macht aus. Ob sie dabei rechtskonform handelt, bemisst sich aber nicht ausschließlich nach den Maßstäben nationalen Rechts. Denn unterdessen steuert die Richtlinie für Polizei und Justiz (JI-RL)[60] die Datenverarbeitung der Polizei.[61] Biometrische Gesichtserkennung bewegt sich damit an der Schnittstelle zwischen mitgliedstaatlichen Vorgaben und Unionsrecht.

1. Rechtfertigungsanforderungen aus der JI-RL

Art. 10 JI-RL erlaubt den Einsatz biometrischer Gesichtserkennungssysteme nur dann, wenn dieser „unbedingt erforderlich“ ist und geeignete „Garantien für die Rechte und Freiheiten der betroffenen Person“ bestehen. Das bedingt nicht nur technisch-organisatorische Maßnahmen,[62] sondern auch rechtliche Verarbeitungsschranken und Betroffenenrechte, die den Schutz der Grundrechte sowie der Interessen der Betroffenen sicherstellen.[63]

Soweit der Einsatz biometrischer Gesichtserkennungssysteme mit einer Entscheidung einhergeht, die *ausschließlich auf einer automatischen Verarbeitung* beruht, erklärt die JI-RL sie sogar für grundsätzlich unzulässig (Art. 11 I JI-RL). Gesichtserkennungssoftware erlässt zwar nicht eo ipso einen Bußgeldbescheid oder eine polizeiliche Verfügung: Bleibt ein Treffer aus, erfolgen keine weiteren Maßnahmen. Sie trifft immerhin aber auf der Grundlage des Abgleichs mit einer Datenbank automatisiert die Entscheidung darüber, ob eine Person auszusondern ist und sich deshalb polizeiliche Maßnahmen anschließen. Alleine diese Aussonderungsentscheidung kann in Ausnahmefällen bereits eine erhebliche beeinträchtigende Wirkung hervorrufen, die den Tatbestand des Art. 11 JI-RL aktiviert.[64]

Das heißt nicht, dass vollständig automatische Gesichtserkennung in solchen Konstellationen unionsrechtlich nicht rechtfertigbar ist. Sie unterliegt aber hohen Rechtfertigungsanforderungen: Zulässig ist diese nur dann, wenn das unionale oder mitgliedstaatliche Recht dies ausdrücklich vorsehen und geeignete Garantien für die Rechte und Freiheiten der betroffenen Person bieten (Art. 11 I JI-RL). Für biometrische Daten als besondere Kategorien personenbezogener Daten sind auch „geeignete Maßnahmen“ zum Schutz der Betroffenenrechte geboten (Art. 11 II JI-RL):[65] Die Behörden müssen Betroffenen zum einen das Recht einräumen, dass der Verantwortliche ggf. persönlich eingreift, sowie über Risiken, Garantien und Rechte informieren und darüber aufklären, wie sie ihre Rechte geltend machen können; zum

51 Bretthauer, Intelligente Videoüberwachung S. 102 f.; dpa, Polizei Mannheim: Smarte Videoüberwachung hilft – „aber kein Allheilmittel“, heise online vom 24.8.2020.

52 Siehe hierzu grundlegend Goodfellow/Bengio et al., Deep Learning, 2016, S. 5 ff.

53 Grother/Ngan et al., Ongoing Face Recognition Vendor Test (FRVT) S. 6, 36 f. m. w. N.

54 Die Fehlerquote von Gesichtserkennung wird typischerweise in der False-Match-Rate und False-Non-Match-Rate gemessen. Erstere beschreibt die Wahrscheinlichkeit, mit der eine Person fälschlicherweise als diejenige Person erkannt wird, deren Daten als Referenzdaten vorliegen. Die Falsch-Zurückweisungsrate bezeichnet die Wahrscheinlichkeit, mit der das System eine Person, deren Daten als Referenzdaten vorliegen, nicht erkennt, obwohl es sich um die richtige Person handelt. Dazu bspw. Schindler, Biometrische Videoüberwachung, S. 171 ff.

55 Siehe bspw. Grother/Ngan et al., Ongoing Face Recognition Vendor Test (FRVT) S. 6 ff., die auch potenzielle Probleme bei hohen Genauigkeitsraten hervorheben und zu dem Ergebnis kommen: „Accuracy of facial recognition implementations varies greatly across the industry“ (9). Vgl. auch Buolamwini/Gebru, Proceedings of Machine Learning Research 81 (2018), 1 (1, 7 f.). Die American Civil Liberties Union hat Amazons Gesichtserkennungssystem einem öffentlichkeitswirksamen Test unterzogen: Sie hat die öffentlich verfügbaren Fotos aller Kongressabgeordneten mit einer US-amerikanischen Fahndungsdatenbank verglichen und 28 falsch-positive Ergebnisse erhalten.

56 Buolamwini/Gebru, Proceedings of Machine Learning Research 81 (2018), 1 (9).

57 Eine weitere wichtige Fehlerquelle für Gesichtserkennungssysteme sind schlecht beleuchtete Fotos oder ungünstige Aufnahmewinkel.

58 Heldt MMR 2019, 285 (286).

59 Vgl. etwa Schesswendter, Gesichtserkennung: Fehler brachte US-Bürger unschuldig ins Gefängnis, t3 n Magazin vom 30.12.2020.

60 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 S. 89, ber. 2018 L 127 S. 9 und 2021 L 74 S. 36).

61 Dient die intelligente Videoüberwachung der Gefahrenabwehr oder der Strafverfolgung, gibt die RL (EU) 2016/680 die datenschutzrechtliche Marschroute vor. In allen anderen Fällen sind die Vorgaben der DSGVO zu beachten.

62 Siehe dazu insbes. etwa die Sicherheitsanforderungen aus Art. 29 II JI-RL.

63 Petri, GSZ 2018, 144 (146).

64 Siehe dazu etwa Martini, in: Paal/Pauly (Hrsg.), DSGVO/BDSG, 3. Aufl., 2021, Art. 22 DSGVO, Rn. 16 a; anders Schindler, Biometrische Videoüberwachung, S. 697 ff.

65 Vgl. insoweit auch allgemeiner Held, Intelligente Videoüberwachung, S. 187; Schindler, Biometrische Videoüberwachung, S. 602 ff.

anderen dürfen die Sicherheitsbehörden nur die benötigten personenbezogenen Daten erheben und nicht länger als für den Verarbeitungszweck erforderlich speichern.[66] Das impliziert insbesondere (regelmäßig zu überprüfende) enge Löschungsfristen.[67]

2. Anwendbarer Grundrechtsmaßstab und grundrechtliche Rechtfertigung

Da das Unionsrecht das Polizeirecht unterdessen nachhaltig sekundärrechtlich überformt, kann sich der Rahmen, in dem sich Gesichtserkennungstechnologie grundrechtlich bewegt, entweder aus dem *unionalen Grundrecht* auf Schutz personenbezogener Daten (Art. 8 GRCh) sowie dem Recht auf Achtung des Privatlebens (Art. 7 GRCh) oder dem Recht auf informationelle Selbstbestimmung (Art. 2 I GG i. V. m. Art. 1 I GG) des *nationalen Verfassungsrechts* ergeben.

Welcher Maßstab greift, bestimmt sich nach Art. 51 I 1 GRCh: Das Handeln der Mitgliedstaaten ist der Grundrechtecharta unterworfen, soweit sie Unionsrecht durchführen. Dafür genügt nicht allein, dass ein nationales Umsetzungsgesetz in den Geltungsbereich des Unionsrechts fällt. Erforderlich ist vielmehr, dass ein unionaler Rechtsakt den Inhalt eines Rechtsgebiets vorgibt, ohne dass den Mitgliedstaaten ein Regelungsspielraum verbleibt. Steht ihnen demgegenüber ein eigener Umsetzungsspielraum zu, gefährdet der nationale Gesetzgeber die einheitliche Anwendung des Rechts der EU als Rechtsgemeinschaft nicht.[68] Die Union lässt dann Raum für Grundrechtsvielfalt, sodass das nationale Verfassungsrecht den Prüfungsmaßstab vorgibt (das aber unionsrechtsfreundlich im Lichte der Grundrechte der Grundrechtecharta auszulegen ist).[69]

Die JI-RL belässt den Mitgliedstaaten einen weiten Spielraum dafür, wie sie ihre regelmäßig sehr abstrakt gehaltenen Vorgaben umsetzen:[70] Sie etabliert erklärtermaßen lediglich *Mindest*standards für polizeiliche Datenverarbeitungen. Den Mitgliedstaaten steht es frei, auf nationaler Ebene höhere Schutzanforderungen zu verankern (Art. 1 III JI-RL). Inwieweit Maßnahmen der Gesichtserkennung zulässig sind, bestimmt sich daher regelmäßig (vorrangig) nach nationalem Verfassungsrecht, allen voran dem Gewährleistungsgehalt des Rechts auf informationelle Selbstbestimmung.[71]

a) Schutzbereich und grundrechtliche Eingriffsintensität

Das Recht auf informationelle Selbstbestimmung aus Art. 2 I i. V. m. Art. 1 I GG schützt den Einzelnen – auch dann, wenn er sich in die Öffentlichkeit begibt – davor, dass der Staat seine persönlichen Daten[72] unbegrenzt erhebt, verarbeitet oder weitergibt.[73] Ein Eingriff entfällt nicht bereits deshalb, weil eine öffentliche Beschilderung auf die (intelligente) Videoüberwachung aufmerksam macht. Wer sich in einen videoüberwachten Bereich begibt, stimmt der Überwachung weder ausdrücklich noch bewusst zu.[74]

Die grundrechtliche Wirkung automatisierter Gesichtserkennung überschreitet in vielfacher Hinsicht eine kritische Schwelle der Sensibilität: Im Unterschied zu bereits länger üblichen Bild- und Tonaufnahmen stellt sie unmittelbar die Verbindung zwischen den über eine Person gesammelten Informationen und ihrer Identität her[75] – ggf. (etwa in Gestalt einer auf die Auswertung gestützten Ingewahrsamnahme) mit unmittelbaren Folgen für die Betroffenen und ihre Verhaltensfreiheit.[76] Die Aufnahmen von Gesichtserkennungskameras beschneiden dadurch besonders stark einen sehr sensiblen Bereich der Persönlichkeit. Schließlich ist das Gesicht das höchstpersönlichste Merkmal,[77] das sich nicht abändern lässt und eine hohe soziale Bedeutung aufweist.[78] Je persönlicher der Anknüpfungspunkt, desto intensiver der Eingriff.

Öffentliche Videoüberwachung mit Hilfe biometrischer Merkmale tangiert nicht zuletzt strukturbedingt die Rechtssphäre zahlreicher Unbeteiligter, gegen die kein konkreter Verdacht besteht. Daten solcher Personen einzubeziehen, deren Abgleich letztlich zu Nichttreffern führt, verleiht der Kontrolle als Fahndungsmaßnahme einerseits gerade ihren tieferen Sinn.[79] Personen, die selbst keinen Anlass für die Kontrolle gesetzt haben, setzt eine solche Überwachungsmaßnahme andererseits dem Gefühl ständigen Überwachtseins aus.[80] Schon kraft dieser Streubreite entfaltet der Eingriff eine hohe Intensität. Selbst dann, wenn die zuständige Stelle die Daten sogleich wieder (automatisiert) löscht bzw. nicht speichert, sie aber nicht lediglich technisch und ungezielt ohne Erkenntnisinteresse miterfasst, greift Gesichtserkennung auch bei Nichttrefferfällen in das Grundrecht auf informationelle Selbstbestimmung ein.[81] Mag die Beeinträchtigung für den Einzelnen in diesem Fall gering sein, so geht von ihr doch ein Einschüchterungseffekt aus, der ab-

66 ErwGr. 26 der JI-Richtlinie (EU) 2016/680.
67 ErwGr. 26 der JI-Richtlinie (EU) 2016/680.
68 Jarass, in: ders. (Hrsg.), EuGRCh, 4. Aufl., 2021, Art. 51, Rn. 25 f.
69 Soweit das Grundgesetz das Schutzniveau der GRCh unterschreitet, ist eine Prüfung allein am Maßstab der deutschen Grundrechte in den Augen des Gerichts nicht ausreichend. Das gilt vor allem dann, wenn der EuGH für ein Unionsgrundrecht einen spezifischen Schutzstandard entwickelt hat, BVerfGE 152, 152 (181 f., Rn. 69). Das BVerfG scheint die Unionsgrundrechte bei Gestaltungsspielräumen als einen Mindeststandard zu interpretieren; das geht nicht unbedingt mit dem eigentlichen Zweck der Unionsgrundrechte konform: Diese sollen keinen grundrechtlichen Basisstandard verbürgen, sondern einen vollwertigen Grundrechtsschutz gewährleisten. Inzwischen hat das BVerfG den Weg beschritten, die Grundrechte des GG, der GRCh und der EMRK zu einem einheitlichen „Beziehungsweise-Maßstab“ (siehe dazu Pustelnik, Drei sind eins und eins sind wir, verfassungsblog.de vom 16.7.2021) zu verbinden (vgl. BVerfG, BeckRS 2021, 12337, Rn. 58 ff.), den das Gericht mit der „weitestgehenden Deckungsgleichheit“ der Grundrechtsregime begründet (Rn. 67).
70 Die DSGVO entfaltet gegenüber den Mitgliedstaaten zwar unmittelbare Wirkung. Innerhalb des normativen Rahmens, den die Verordnung zeichnet, räumt sie den Mitgliedstaaten für den Bereich hoheitlichen Tätigwerdens ihrer Sicherheitsbehörden aber via Öffnungsklauseln einen weiten Handlungsspielraum ein (z. B. Art. 6 I lit. e, II und III, Art. 9 II lit. g, Art. 10, Art. 17 III 3 lit. b, Art. 23, 36 V, Art. 49 I 1 lit. d i. V. m. IV, V DSGVO). Dazu Kühling/Martini et al., Die DSGVO und das nationale Recht, 2016, S. 9 ff.
71 Dieses Grundrecht ist jedoch im Lichte der GRCh auszulegen, sofern der EuGH für die Norm einen spezifischen Schutzstandard entwickelt hat.
72 BVerfGE 65, 1 (43).
73 BVerfGE 150, 244 (264 f.); BVerfGE 120, 378 (399).
74 BVerfG NVwZ 2007, 688 (690) m. w. N.; Kulick, NVwZ 2020, 1622 (1624).
75 Auch insoweit entsprechen die automatisierte Erhebung und der Abgleich dem Ablauf bei der automatisierten Kennzeichenüberwachung, so dass die entsprechenden Anforderungen des BVerfG (BVerfGE 150, 244 ff.) übertragbar sind.
76 Dass es unklar ist, ob diese Folgen eintreten, ändert nichts daran, dass die Gesichtserkennung als solche bereits freiheitsbeeinträchtigend ist; BVerfGE 150, 244 (268 f.).
77 BVerfGE 150, 244 (269).
78 Zur generellen Problematik biometrischer Informationen, von denen sich ein Mensch nicht (oder nur schwer) lösen kann, vgl. Commission Nationale de l´Informatique et des Libertés (CNIL), Facial recognition: for a debate living up to the challenges, S. 6.
79 BVerfGE 150, 244 (267 f.).
80 BVerfGE 150, 244 (267 f.).
81 Es gilt insoweit Gleiches wie im Falle automatischer Kennzeichenerfassung, vgl. BVerfGE 150, 244 (266 ff.). „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“ (aaO, 267 f.). Ebenso etwa Schindler, Biometrische Videoüberwachung, S. 324 f.

schreckend wirken kann. Denn zu dem Zeitpunkt, zu dem die Kamera die Gesichtsdaten erhebt, hat sich das behördliche Interesse an den Daten *aller* Betroffenen bereits verdichtet.[82]

Anders als im Falle einer herkömmlichen Identitätsfeststellung durch Polizeibeamte kann der Einzelne auch nicht ohne Weiteres einschätzen, welche Berechnungen die Software über ihn im Detail vornimmt. Nicht jeder Betroffene überblickt, für welche Zwecke staatliche Behörden sein Gesicht erfassen und auf welche Kontexte sich dieses Instrumentarium beschränkt. Unter Umständen bemerkt er gar nicht, dass ein System im Hintergrund automatisiert konkrete Verdachtsmomente überprüft. Indem Gesichtserkennung den Fahndungsaufwand substanziell verringert, der erforderlich ist, um eine Person zu identifizieren,[83] senkt sie auch die Hemmschwelle, Individuen, die sich im öffentlichen Raum bewegen, zu identifizieren und algorithmisch durchzuspielen, ob von ihnen eine Gefahr ausgehen könnte. Was den Ermittlungsradius der Sicherheitsbehörden ausweitet und Sicherheitsbedürfnisse erfüllt, schränkt reflexartig den Freiheitsraum der Bürger ein.[84] Speichert die Polizei die Aufnahmen, vertieft das den Eingriff zusätzlich: Die zuständigen Stellen können dann technisch in weiteren Bearbeitungsschritten Querverbindungen zwischen unterschiedlichen Informationen und Datenbeständen herstellen und dadurch im Extremfall das Tor zu einer umfassenden staatlichen Profilbildung des Bürgers aufstoßen.[85]

b) Rechtfertigungsanforderungen

Das Recht auf informationelle Selbstbestimmung genießt zwar besonderen verfassungsrechtlichen Schutz. Es ist aber kein absolutes Recht. Der Gesetzgeber darf es beschränken. Will er biometrische Gesichtserkennung als Instrument zulassen, muss er dafür jedoch eine gesetzliche Eingriffsgrundlage aus der Taufe heben, die im Grad ihrer Bestimmtheit sowie der inhaltlichen Regelungsdichte der Intensität des Eingriffs entspricht.[86] In einer normenklaren Weise[87] hat der Gesetzgeber Anlass, Zweck und Grenzen des Einsatzes biometrischer Gesichtserkennung so bestimmt festzulegen, dass der Verwaltung daraus klare Handlungsmaßstäbe erwachsen.

aa) Die automatisierte Kennzeichenkontrolle als Vergleichsfall

Wie hoch die Rechtfertigungsanforderungen an das polizeiliche Werkzeug der Gesichtserkennung liegen, lässt sich durch einen Vergleich zu anderen Referenzkonstellationen – insbesondere zur automatisierten Kennzeichenkontrolle – annäherungsweise ermessen.

Mit ihr teilt Gesichtserkennung kraft ihrer Streubreite und funktionstypischen Logik zahlreiche strukturelle Gemeinsamkeiten: Beide zielen darauf, den öffentlichen Raum automatisiert zu überwachen. Sie erheben personenbezogene Merkmale und gleichen diese – verdachtsunabhängig – mit einer Datenbank ab. Die Polizei kann mit ihrer Hilfe technisch nicht nur auf das Bewegungsverhalten, sondern auch auf das sonstige Verhalten der erfassten Personen rückschließen – namentlich dann, wenn Bewegungsprofile entstehen.[88] Angesichts ihrer Verknüpfungsmöglichkeiten lassen sich beide Instrumente im Grundsatz als technisches Mittel dauerhafter Observation einsetzen.[89]

Da die rechtlichen Hürden für eine automatische Kennzeichenerfassung bereits hoch liegen,[90] sind sie für biometrische Gesichtserkennungssysteme umso höher anzusetzen. Denn während Kfz-Kennzeichen keinen unmittelbaren, sondern nur einen mittelbaren Rückschluss auf persönliche Merkmale und die Identität der Betroffenen zulassen,[91] misst biometrische Gesichtserkennung sensible Gesichtsdaten der Betroffenen aus und zieht diese als Anknüpfungspunkt zur Identifizierung heran. Hinzu tritt das Risiko diskriminierender Fehleinschätzungen, die an die Ethnie, das Geschlecht oder andere Merkmale der betroffenen Personen anknüpfen.[92] Nicht zuletzt potenziert die immer größer werdende Menge sensibler Daten, die die zuständigen Stellen via Gesichtserkennung nunmehr in kürzester Zeit technisch auswerten (können), die Eingriffsintensität: Aus der Quantität der Daten erwächst eine neue Qualität des Eingriffs in das Recht auf informationelle Selbstbestimmung.[93] Eine abstrakte bzw. „typisierte Gefahr" genügt daher nicht als eingriffsrechtfertigender Tatbestand: Eine Kontrolle beliebiger Orte „ins Blaue hinein" ist nicht zulässig.[94] Vielmehr muss die Maßnahme durch einen konkreten, objektiv bestimmbaren Grund veranlasst sein.[95] Auch das allgemeine Interesse, nach bestimmten Personen zu fahnden, reicht nicht, um eine intelligente Videoüberwachung zu legitimieren.[96]

bb) Totalüberwachung als rote Linie

Eine rote Linie überschreitet der Einsatz von Gesichtserkennungssoftware jedenfalls dann, wenn er in eine „Totalüberwachung" der Bürger umschlägt,[97] also keine wesentlichen überwachungsfreien Räume mehr verbleiben. Dafür reicht eine „nahezu lückenlos[e]" Registrierung und Katalogisierung als Grundlage für Persönlichkeitsprofile bereits aus.[98] Selbst in allen Fällen der Wohnraumüberwachung[99] und Vorratsdatenspeicherung[100] hat das BVerfG diese kritische

82 BVerfGE 150, 244 (267 f.).
83 Dadurch verkehrt sich ein Stück weit auch die Fahndungslogik: Ist die Identität aller Personen, die sich im öffentlichen Raum aufhalten, (potenziell) bekannt, fällt es leichter, an sie mögliche Gefahren anzuknüpfen, als für ausgemachte Gefahren nach Verursachern zu suchen. Die Gefahr, dass es zu Vorverurteilungen und falschen Zuordnungen kommt, steigt dadurch beträchtlich.
84 Ist eine Person einmal als Individuum ausgemacht, fällt es umso leichter, sie zu überwachen und mit staatlichen Maßnahmen zu konfrontieren – von der erzieherisch intendierten Prangerwirkung für jemanden, der eine rote Ampel überquert (wie in China praktiziert), bis hin zu konkreten Sanktionen für Personen, die sich etwa regelmäßig in einem berüchtigten Viertel aufhalten.
85 BVerfG NVwZ 2007, 688 (690).
86 Vgl. auch BVerfG NVwZ 2007, 688 (690) mwN.
87 BVerfGE 120, 378 (407 f.); BVerfGE 150, 244 (278 f.).
88 BVerfGE 120, 378 (405 f.).
89 Deren „besondere Schlagkraft und Eingriffsintensität [erwächst] auch aus den durch die Automatisierung und Vernetzung ermöglichten verbesserten Bedingungen für eine effektive und zudem heimliche Datenerfassung und -verarbeitung"; BVerfGE 120, 378 (406 f.).
90 Eine flächendeckende automatisierte Kontrolle mit Datenerhebung ist ebenso wenig zulässig, wie technische Geräte dauerhaft zu diesem Zweck einzurichten, BVerfGE 150, 244 (285, 289). Die Überwachung darf daher nur punktuell und zeitlich befristet erfolgen, BVerfGE 120, 378 (407 ff.).
91 BVerfGE 150, 244 (283, Rn. 97).
92 Siehe dazu oben II. 3.
93 BVerfGE 120, 378 (397 f.); Kulick NVwZ 2020, 1622 (1624).
94 BVerfGE 150, 244 (288 f.). Anlasslose Kontrollen sind nicht generell ausgeschlossen; sie sind möglich, wenn sie etwa an typisch gefährliches oder risikobehaftetes Tun anknüpfen und stichprobenhaft erfolgen (aaO, 282, Rn. 94).
95 Vgl. BVerfGE 150, 244 (280 ff.); ausreichend sind auch „Gefahrenlagen […], die nur typisiert umschrieben sind" (Rn. 93); zu anlasslosen Kontrollen, vgl. Rn. 94.
96 BVerfGE 150, 244 (281).
97 St. Rspr., BVerfGE 65, 1 (42 f.); 109, 279 (323); 112, 304 (319); 125, 260 (323 f.); 130, 1 (24); vgl. auch Desoi, Intelligente Videoüberwachung, S. 71; Roßnagel NJW 2010, 1238 (1240).
98 BVerfGE 109, 279 (323); 130, 1 (24); Desoi, Intelligente Videoüberwachung, S. 72.
99 BVerfGE 130, 1 (24 f.).
100 BVerfGE 125, 260 (321 f.).

Grenze zur Totalüberwachung jedoch nicht als überschritten angesehen.[101]

Staatliche Überwachungsinstrumente sind zugleich nicht isoliert zu betrachten. Es ist vielmehr eine *Gesamtschau* aller Werkzeuge vorzunehmen.[102] Die intelligente Videoüberwachung kann einen Baustein eines Gesamtsystems additiver Grundrechtseingriffe[103] (etwa neben automatischer Kennzeichenerfassung, Vorratsdatenspeicherung etc.) bilden, die in ihrer Summe in eine unzulässige Belastungskumulation münden.[104]

Gesichtserkennung muss als Teil des Gebots der Angemessenheit nicht nur inhaltlich, räumlich und zeitlich beschränkt sein, sondern als Ausfluss eines Grundrechtsschutzes durch Verfahren auch hinreichenden *verfahrensrechtlichen Beschränkungen* unterliegen, die dem Einsatz der Technologie klare Grenzen ziehen.[105] Die gesetzliche Eingriffsgrundlage[106] muss namentlich *Transparenz* über potenzielle Einsatzszenarien, *individuellen Rechtsschutz* und *aufsichtsrechtliche Kontrolle* gewährleisten.[107] Etwaige Maßnahmen muss die Behörde protokollieren, um die Rechtmäßigkeit, Nachvollziehbarkeit und Überprüfbarkeit der Verwaltungsentscheidung sicherzustellen.[108]

IV. Gesichtserkennung im einfachen Recht de lege lata

Welche rechtlichen Anforderungen an Maßnahmen automatisierter Gesichtserkennung in concreto zu stellen sind, bestimmt sich insbesondere nach der Art des Einsatzszenarios, in dem sie zur Anwendung gelangt. Unter den Spielarten der Echtzeiterkennung lässt sich idealtypisch zwischen dem anlasslosen, dauerhaften Einsatz (1.), dem zweckspezifischen, zeitlich begrenzten Einsatz (2.) sowie dem anlassbezogenen, nicht dauerhaften Einsatz biometrischer Identifizierungsverfahren, etwa zur Einlasskontrolle gefährdeter Orte (3.), unterscheiden.

1. Anlasslose, dauerhafte Gesichtserkennung (Fallkonstellation Berlin Südkreuz)

Paradefall einer dauerhaften, anlasslosen und in Echtzeit erfolgenden Gesichtserkennung ist der Pilotversuch, den die Bundespolizei am Bahnhof Berlin Südkreuz unternommen hat.[109] Er zielte darauf, das kamerabasierte Identifizierungssystem mit Hilfe der Gesichter vorbeilaufender Personen darauf zu trainieren, möglichst fehlerfrei jene herauszufiltern, die als gesucht in einer Datenbank hinterlegt sind.

a) Präventivpolizeiliche Zwecksetzung

aa) Spezielle Ermächtigung zur intelligenten Videoaufnahme in Bundes- und Landesgesetzen?

Für die Überwachung am Bahnhof Berlin Südkreuz scheint prima facie § 27 S. 1 Nr. 2 BPolG als Eingriffsgrundlage prädestiniert.[110] Die Norm ist sehr weit gefasst: Sie gestattet im Bereich von Bahnhöfen, Flughäfen und Grenzgebieten zum Zwecke der Gefahrenabwehr selbsttätige Bildaufnahme- und Bildaufzeichnungsgeräte, die das Geschehen ohne menschliches Zutun aufzeichnen.[111] Der Wortlaut der Regelung fordert insbesondere nicht ausdrücklich einen spezifischen Anlass.[112] Statt einer konkreten Gefahr lässt er schon die bloße Ermittlung einer möglichen Gefahr ausreichen.

Dass die Rationalität der Norm auch einen – automatisiert und dauerhaft erfolgenden, anlasslosen – Einsatz von Gesichtserkennungssystemen deckt, ist damit aber nicht gesagt.[113] Denn die dauerhafte automatische Gesichtserkennung an bestimmten öffentlichen Orten entwickelt die herkömmliche Videoüberwachung nicht lediglich linear weiter. Mit ihrer besonderen Eingriffsintensität hebt sie die staatliche Maßnahme vielmehr auf eine neue Stufe eigener Qualität.[114] § 27 S. 1 Nr. 2 BPolG etabliert insbesondere keine flankierenden gesetzlichen Regelungen, um die spezifischen Risiken einer automatisierten Gesichtserkennung einzudämmen und das grundrechtliche Gefährdungspotenzial auf ein rechtsstaatlich vertretbares Maß zu beschränken. So mangelt es an konkreten gesetzlichen Vorgaben zum zulässigen Anlass der Überwachung, den verknüpften Datenbanken oder zu gebotenen Verfahrenssicherungen. Je intensiver der Eingriff, um so bestimmter und klarer muss die Eingriffsgrundlage das rechtlich Erlaubte aber benennen. Die offenen Tatbestandsvoraussetzungen der Norm reichen deshalb nicht

101 Desoi, Intelligente Videoüberwachung, S. 72.
102 So die überzeugende Folgerung von Desoi, Intelligente Videoüberwachung, S. 73 und Roßnagel, NJW 2010, 1238 (1240) aus dem Vorratsdatenspeicherungsurteil des BVerfG. Zur Überwachungsgesamtrechnung auch Schindler, Biometrische Videoüberwachung, S. 618 ff. Ein Projekt des Max-Planck-Instituts zur Erforschung von Kriminalität, Sicherheit und Recht hat es sich zur Aufgabe gemacht, die „reale Überwachungslast" zu untersuchen, siehe Poscher/Kilchling, Entwicklung eines periodischen Überwachungsbarometers für Deutschland, 2021, S. 2 ff.
103 BVerfGE 112, 304 (319); Schindler, Biometrische Videoüberwachung, S. 638 ff.
104 Desoi, Intelligente Videoüberwachung, S. 74, 76, 96 ff.; vgl. auch Schaks DÖV 2015, 817 (819); Martini, in: Paal/Pauly (Hrsg.), Art. 22 DSGVO, Rn. 16 a; aA Held, Intelligente Videoüberwachung S. 114 f.
105 BVerfGE 150, 244 (283). Dies gilt insbesondere dann, wenn Polizeibehörden und Nachrichtendienste eine gemeinsame Datenbank nutzen (entsprechend der zentralen Antiterrordatei), siehe BVerfG NVwZ 2021, 226 (231, Rn. 85 ff.).
106 Eine Generalklausel, die nur eine polizeirechtliche Gefahr zur Voraussetzung macht, genügt bei Datenverarbeitungen nicht, vgl. BVerfGE 150, 244 (286, Rn. 106).
107 BVerfGE 65, 1 (44 ff.); 125, 260 (334 ff.); 141, 220 (282); 150, 244 (285 m. w. N.); Vgl. auch Bretthauer, Intelligente Videoüberwachung, S. 50 f. mwN.
108 BVerfGE 150, 244 (278 f.).
109 Siehe dazu oben IV. 1.
110 Die Bundesregierung hat sich in dem Testprojekt Südkreuz auf diese Norm berufen, BT-Drs. 19/3750, S. 5. Von Testpersonen hat die Bundespolizei schriftliche Einwilligungen eingeholt und alle den Bereich durchschreitenden Personen mit einer ausschließlich aus diesen Testpersonen bestehenden Datenbank verglichen; siehe Abschlussbericht Gesichtserkennung, S. 20 ff. abrufbar unter https://www.bundespolizei.de/Web/DE/04Aktuelles/01Meldungen/2018/10/181011_abschlussbericht_gesichtserkennung.html. Eine Einwilligung in eine Gesichtserkennung ist rechtlich möglich, da diese nicht unzulässig in die Menschenwürde eingreift und die Entscheidungsfreiheit die objektivrechtliche Schutzanordnung überwiegt, im Ergebnis BT-Drs. 19/5011, S. 3; allgemein zu zulässigen Einwilligungen in Eingriffe in das allgemeine Persönlichkeitsrecht vgl. BVerfGE 106, 28 (44 ff.); Di Fabio, in: Dürig/Herzog/Scholz (Hrsg.), GG, 95. Erg.-Lfg (Juli 2021), Art. 2 Abs. 1, Rn. 228; Starck, in: Mangoldt/Klein/Starck (Hrsg.), 7. Aufl., 2018, Art. 1 GG, Rn. 300, 114. Vgl. auch https://www.bfdi.bund.de/DE/Infothek/Pressemitteilungen/2017/15_BiometrischeGesichterkennungSuedkreuz.html. Das System konnte die sonstigen Passanten zwar nicht identifizieren. Das ändert aber nichts daran, dass es einer gesetzlichen Grundlage bedarf, um ihre Daten mittels Gesichtserkennung zu verarbeiten. Der verbleibende Eingriff des Filmens der sonstigen Passanten muss sich an der Norm des § 27 S. 1 Nr. 2 BPolG messen lassen, BT-Drs. 19/5011, S. 3.
111 Siehe dazu bspw. Brunner, Grundrechtsfragen beim Einsatz von Kampfdrohnen durch die Bundeswehr im Ausland, in: Frau (Hrsg.), Drohnen und das Recht, 2014, S. 163, § 27, Rn. 1; Wehr, in: ders. (Hrsg.), BPolG, 2. Aufl., 2015, § 27, Rn. 1.
112 Ein solcher ist selbst für Kennzeichenkontrollen erforderlich (BVerfGE 150, 244 [280 ff., Rn. 89 ff.]). In manchen Konstellationen kann sich dieser Anlass bereits aus der besonderen Gefährlichkeit einer Tätigkeit oder der Beherrschung einer Gefahrenquelle ergeben. Kontrollen, die keinem spezifischen Anlass geschuldet sind, sind in dieser Lesart nicht gänzlich unzulässig. Siehe zu diesem Aspekt auch ausführlich oben III. 2. b) aa).
113 Eine Anwendung auf intelligente Videoüberwachung ablehnend: Heldt, MMR 2019, 285 (287); zur Diskussion vgl. Wiss. Dienst des dt. Bundestages, Rechtsgrundlage für den Einsatz sog. intelligenter Videoüberwachung durch die Bundespolizei, WD 3 – 3000 – 202/16.
114 Vgl. Heldt MMR 2019, 285 (287). Siehe auch III. 2. a).

aus, um automatische Echtzeit-Gesichtserkennungssoftware als staatliches Identifizierungsinstrument zu decken. Auch die Begründung zum Gesetzentwurf erhellt, dass der historische Gesetzgeber selbst eine solche Technik nicht erwogen hat und sie jedenfalls nicht in diesem tiefgehenden Umfang legitimieren wollte.[115]

Auf die derzeit existierenden *landesrechtlichen* Vorschriften, die es der Polizei allgemein gestatten, Bild- und Videoaufnahmen anzufertigen und zu verarbeiten (so etwa § 18 I, III, V HmbPolDVG n. F.[116]), lässt sich eine anlasslose, dauerhafte Gesichtserkennung ebenfalls nicht stützen. Ratione materiae adressieren die Vorschriften Aufzeichnungen einer Kamera, die ein *Mensch* in Echtzeit oder im Anschluss an ein Ereignis analysiert. Selbst soweit die bestehenden Regelungen „technikoffen" ausgestaltet sind,[117] also keine bestimmte Form der Bildaufzeichnung vorgeben, ist jedenfalls für den automatisierten Abgleich biometrischer Daten mit einer Datenbank eine spezifische Rechtsgrundlage erforderlich. Das gebietet die besondere grundrechtliche Sensibilität des neuen Überwachungssystems, das die herkömmliche Videoüberwachung mit einer softwarebasierten Analyse der Aufnahmen sowie einem Abgleich mit einer polizeilichen Datenbank kombiniert.[118] Die Vorschriften konturieren den Anlass, den Zweck und die Grenzen eines für die Gesichtserkennung erforderlichen automatisierten Datenbankabgleichs ebenso wie § 27 S. 1 Nr. 2 BPolG aber nicht in hinreichendem Maße.

Hessen (§ 25 a HSOG) sowie die Freie und Hansestadt Hamburg (§ 49 HmbPolDVG) gestatten ihrer Polizei immerhin, auch eine automatisierte Datenauswertung solcher personenbezogenen Daten vorzunehmen, die in polizeilichen Dateisystemen gespeichert sind.[119] Die Vorschriften sollen insbesondere dazu beitragen, Straftaten im Bereich des internationalen Terrorismus bzw. der schweren und organisierten Kriminalität durch Datenabgleich zu verhindern bzw. aufzuklären.[120] Sowohl in Hessen als auch in Hamburg erlaubt die Norm, Daten aus verschiedenen Quellen zusammenzuführen, nicht aber neue Daten zu erheben – erst recht nicht biometrische Daten mittels Gesichtserkennung.[121] Die Eingriffsgrundlagen sprechen lediglich von *gespeicherten personenbezogenen Daten* (§ 25 a I 1 HSOG; § 49 I 1 HmbPolDVG), nicht aber von der *Erhebung biometrischer Daten*, wie sie für die Gesichtserkennung Voraussetzung sind. Entsprechend dem Grundsatz der Normenklarheit muss eine Vorschrift, die Gesichtserkennung legitimieren soll, aber gerade auch die spezifische Einsatztechnik hinreichend klar benennen. Dieser Anforderung genügen die Regelungen zum Datenabgleich nicht.

Erst recht lässt sich Gesichtserkennung mit Blick auf ihre Eingriffsintensität und Streubreite nicht auf die *Datenerhebungs-Generalklausel* der Polizeigesetze der Länder bzw. § 21 BPolG stützen.[122] Umfangreiche, dauerhafte und automatische Datenbankabgleiche, die eine Vielzahl von Grundrechtsträgern betreffen, erfordern eine konkrete Eingriffsgrundlage, die Vorgaben für den Anlass, die konkret abzuwehrende Gefahr und Verfahrenssicherungen explizit im Gesetz verankert. Die polizeilichen Datenerhebungs-Generalklauseln bleiben hinter diesen gesteigerten Anforderungen an Normenbestimmtheit und Normenklarheit[123] weit zurück.

bb) § 48 BDSG

Neben den Fachgesetzen hält auch das BDSG Rechtsgrundlagen bereit, die es Polizeibehörden gestatten, biometrische Daten unter spezifischen Voraussetzungen zu erheben und zu verarbeiten.[124] Auf § 48 BDSG[125] hat namentlich das VG Hamburg die Maßnahmen der Gesichtserkennung gestützt, welche die Polizei im Nachgang zu den G20-Ausschreitungen vorgenommen hat.[126] Die Vorschrift regelt, inwieweit Polizeibehörden besondere Kategorien personenbezogener Daten, insbesondere biometrische Daten, verarbeiten dürfen. Ebenso wie die polizeirechtlichen Regelungen erweist sich

115 BR-Drs. 417/94, S. 59 (dazu auch Wiss. Dienst des dt. Bundestages, Rechtsgrundlage für den Einsatz sog. intelligenter Videoüberwachung durch die Bundespolizei, WD 3 – 3000 – 202/16, S. 3 f.). Auch die Bundesregierung sprach sich im Rahmen des Testprojekts Berlin Südkreuz im Falle der „Einführung der intelligenten Videotechnik im Wirkbetrieb […], […] [dafür aus, eine] […] bereichsspezifische[.] Rechtsgrundlage [zu schaffen], die die Voraussetzungen und Grenzen für einen Einsatz intelligenter Videoüberwachung auch ohne Einwilligung regelt" (BT-Drs., 19/5011, S. 4). Das ist auch richtig. Denn die automatisierte Auswertung erschöpft sich nicht lediglich in einem Annex zur gesetzlich ausdrücklich zugelassenen selbsttätigen Bildaufnahme.

116 Gesetz vom 12.12.2019, HmbGVBl. 2019 I, S. 485.

117 Ein solches Verständnis ist Ausfluss des Grundsatzes der effektiven Gefahrenabwehr, vgl. etwa Martini DÖV 2019, 732 (736). Zu den Grenzen dieser Auslegung bspw. BVerfGE 112, 304 (315 ff.); Roggan NJW 2015, 1995 (1999).

118 Dass § 19 HmbPolDVG die automatisierte Kennzeichenerfassung gesondert regelt, illustriert paradigmatisch, dass § 18 HmbPolDVG den automatisierten Datenabgleich gerade nicht umfassen soll, sondern es gesonderter Regelungen bedarf, vgl. auch Höhn/Wassermann, Gesichtserkennung in der Öffentlichkeit – Wäre automatisierte Gesichtserkennung im öffentlichen Raum zulässig?, Recht und Netz vom 4.9.2020.

119 Art. 33 V BayPAG gestattet der Polizei ausdrücklich, „Systeme zur automatischen Erkennung und Auswertung von Mustern" einzusetzen. Die Vorschrift beschränkt diese Maßnahme aber auf „Gegenstände", lässt also eine Gesichtserkennung bewusst nicht zu. Ähnliches gilt für § 44 IV 2 BWPolG: Die automatische Auswertung muss sich auf die Verhaltensmustererkennung beschränken.

120 In Hessen zielt die Rechtsgrundlage vor allem auf die Software „HessenDATA" (Gotham) des US-Konzerns „Palantir Technologies Inc.", welche die hessischen Polizeipräsidien und das LKA einsetzen. Die Software erhebt keine neuen Daten. Sie wertet vielmehr „in begründeten Einzelfällen" große Mengen bereits – rechtmäßig – erhobener personenbezogener Daten verschiedener Quellen zentral und automatisiert aus. Dabei kann die Polizei die Daten im Einzelfall von öffentlichen und nicht-öffentlichen Stellen anfordern (§ 26 HSOG). Diese Zusammenführung von Daten aus verschiedenen Quellen – auch wenn sie bereits erhoben waren oder der Bürger sie freiwillig und öffentlich, etwa auf Social-Media-Accounts, ins Internet lud – greift tief in das informationelle Selbstbestimmungsrecht ein und bedarf daher einer spezifischen Rechtsgrundlage.

121 Derzeit ist gegen die Vorschrift eine Verfassungsbeschwerde beim BVerfG anhängig. Sie soll klären, ob § 25 a HSOG mit Blick auf seine hohe Eingriffsintensität verhältnismäßig ist und ausreichende Verfahrenssicherungen vorsieht.

122 Vgl. bspw. Mysegades NVwZ 2020, 852 (856) m. w. N.

123 Zur Normenklarheit und -bestimmtheit, siehe bspw. BVerfGE 110, 33 (53 ff.).

124 Das BDSG ist nur dann anwendbar, wenn andere Fachgesetze den Sachverhalt nicht oder nicht abschließend regeln (§ 1 II 1 und 2). Das BPolG eröffnet der Bundespolizei in den §§ 21 ff. zwar bereits Möglichkeiten, personenbezogene Daten zu erheben und zu verarbeiten, um die Gefahrenabwehr zu unterstützen. § 48 BDSG findet neben diesen Vorschriften jedoch ergänzend Anwendung. Dies ergibt sich zum einen aus einem Umkehrschluss aus § 37 BPolG: Er erklärt spezifische Normen des BDSG für Aufgaben der Bundespolizei für nicht anwendbar. Der Normgeber bringt dadurch zugleich zum Ausdruck, dass die Normen des BDSG im Grundsatz Anwendung finden. Zum anderen handelt es sich bei § 48 BDSG um eine Spezialregelung für die Verarbeitung besonderer Kategorien personenbezogener Daten. Die Normen des BPolG kennen diesen Zuschnitt auf eine spezielle Datenart nicht, obwohl dies unionsrechtlich geboten ist – und sind deshalb auch materiell nicht abschließend. Bei Tätigwerden der Landespolizei sind zusätzlich die Anforderungen des § 1 I 1 Nr. 2 BDSG zu beachten.

125 § 48 BDSG ist jedoch wie auch seine Parallelnorm Art. 9 DS-GVO – anders als das Gericht meint – keine eigenständige Verarbeitungsgrundlage. Die Norm stellt vielmehr nur zusätzliche Rechtmäßigkeitsvoraussetzungen auf, Frenzel, in: Paal/Pauly (Hrsg.), DSGVO/BDSG, 3. Aufl., 2021, § 48 BDSG, Rn. 4; aA BR-Drs. 110/17, S. 113 f.; Albers, in: Wolff/Brink (Hrsg.), BeckOK DatenschutzR, 37. Ed. (Stand: 1.5.2020), § 48 BDSG, Rn. 13; Braun, in: Gola/Heckmann (Hrsg.), 13. Aufl., 2019, § 48 BDSG, Rn. 1; Schwichtenberg, in: Kühling/Buchner (Hrsg.), DS-GVO/BDSG, 3. Aufl., 2020, § 48 BDSG, Rn. 1.

126 VG Hamburg, 23.10.2019 – 17 K 203/19, BeckRS 2019, 40195, Rn. 86 ff. (v. a. 89 f.).

die Norm aber nicht als hinreichend bestimmt genug,[127] um eine anlasslose und dauerhafte polizeiliche Echtzeitgesichtserkennung[128] bzw. einen Eingriff mit einer derartigen Streubreite zu tragen.[129] Sie schweigt sich insbesondere zu den Zielen und Zwecken der Verarbeitung sowie der Art der verarbeiteten Daten aus.[130] Ebenso wenig steckt sie Grenzen für den Umfang, die Dauer und den Anlass des Eingriffs ab. Auch Verfahrenssicherungen (bspw. mit Blick auf den Datenbankzugriff) kennt die Norm nicht. Diese sind aber für einen derart gravierenden Eingriff unabdingbar. § 48 BDSG lässt zudem technische Anforderungen vermissen, die die Software erfüllen muss bzw. nicht erfüllen darf. Schon deshalb vermag sie eingriffsintensive Maßnahmen wie die Gesichtserkennung nicht zu legitimieren.

cc) § 4 BDSG

Auch § 4 I 1 Nr. 1 BDSG hält eine Erlaubnisnorm für die Videoüberwachung vor. Die Vorschrift lässt eine Beobachtung „mit optisch-elektronischen Einrichtungen" zu, um die Aufgaben öffentlicher Stellen zu erfüllen.[131] Ihre abstrakt gehaltenen tatbestandlichen Vorgaben genügen jedoch (ebenso wie § 48 BDSG) zum einen nicht den (Bestimmtheits-)Anforderungen, die an einen Eingriff dieser Intensitätsstufe zu stellen sind;[132] zum anderen ermächtigt die Vorschrift nicht dazu, *besondere personenbezogene* Daten zu verarbeiten.[133] Das ergibt sich im Umkehrschluss aus § 48 BDSG. Diese Norm regelt in der Binnensystematik des BDSG *spezialgesetzlich*, inwieweit die Polizei besondere personenbezogene Daten verarbeiten darf. Der Rückgriff auf § 4 BDSG ist damit gesperrt.

b) Strafprozessuale Zwecksetzung

Gesichtserkennung kann nicht nur *präventive* Zwecke verfolgen, sondern auch gesuchte Tatverdächtige ausfindig machen und damit *Strafverfolgung* betreiben. Ebenso wie die Vorschriften des BDSG ermächtigt jedoch keine der strafprozessualen Eingriffsgrundlagen dazu, Echtzeit-Gesichtserkennung dauerhaft und anlasslos einzusetzen.[134]

aa) § 81 b Var. 1 StPO

§ 81 b Var. 1 StPO gestattet erkennungsdienstliche Maßnahmen, die ihrer Natur nach auch an biometrische Merkmale einer Person anknüpfen; die Vorschrift beschränkt diese Eingriffsbefugnis jedoch explizit auf Beschuldigte: Sie setzt voraus, dass der Beschuldigte bereits identifiziert ist. Die Erlaubnisnorm soll nicht dazu dienen, Beschuldigte aufzuspüren, sondern konkrete Ermittlungsmaßnahmen legitimieren, die sich auf eine bereits individualisierte Person beziehen, gegen die mindestens ein Anfangsverdacht besteht. Gesichtserkennungsmaßnahmen, die dem Zweck dienen, gesuchte Personen zu identifizieren, deckt die Norm daher nicht.

bb) §§ 100 h I 1, 163 f StPO

§ 100 h I 1 StPO gesteht den Strafverfolgungsbehörden die Handlungsmacht zu, für Observationszwecke bestimmte Mittel, insbesondere herkömmliche Videoüberwachung im Rahmen der Ermittlung konkreter Straftaten einzusetzen („Bildaufnahmen hergestellt werden" bzw. „sonstige besondere für Observationszwecke bestimmte technische Mittel verwendet werden"[135]).[136] Die Vorschrift setzt jedoch – ebenso wie § 81 b Var. 1 StPO – grundsätzlich voraus, dass der einer konkreten Tat Beschuldigte bereits ermittelt ist. Das macht § 100 h II 1 StPO deutlich: Gegen andere Personen darf sich eine Maßnahme für Observationszwecke grundsätzlich nicht richten.[137]

§ 100 h III bzw. § 163 f II 1 StPO lässt zusätzlich Observationen dann zu, „wenn Dritte unvermeidbar betroffen werden". Das rechtfertigt es nach dem Sinn der Vorschrift allerdings nicht, mithilfe von Gesichtserkennung eine allgemeine Verdachtsüberwachung zu betreiben, um gleichsam die Stecknadel im Heuhaufen ausfindig zu machen.

cc) § 163 b II 1 StPO

§ 163 b II 1 StPO ermöglicht, die Identität auch solcher Personen festzustellen, gegen die *kein Tatverdacht* vorliegt. Alle Personen auf dem Bahnhofsgelände anlasslos zu identifizieren, um unter ihnen einen möglichen Straftäter ausfindig zu machen, lässt sich jedoch nicht mehr unter das Merkmal „zur Aufklärung einer Straftat geboten"[138] rubrizieren und ist unverhältnismäßig im Sinne des § 163 b II 2 StPO. Die geringe Wahrscheinlichkeit, durch die Maßnahme gleichsam zufällig einen Verdächtigen aufzufinden, vermag eine Gesichtserkennung angesichts ihrer erheblichen grundrechtlichen Eingriffswirkung ebenso wenig wie im Falle des § 100 a I 1 StPO zu rechtfertigen.[139]

dd) § 98 c StPO

Das Bedürfnis, einen maschinellen Abgleich von Massendaten zuzulassen, um eine Straftat aufzuklären, hat der Gesetzgeber durchaus erkannt und lässt daher in § 98 c StPO eine derartige Maßnahme ausdrücklich zu. Gesichtserkennungssoftware nimmt einen solchen maschinellen Abgleich vor, indem sie biometrische Daten einer Kamera mit den personenbezogenen Daten aus anderen Strafverfahren auf

127 Zu den Bestimmtheitsanforderungen an Normen siehe BVerfGE 123, 39 (78); EuGH, C-362/14, ECLI:EU:C:2015:650, NJW 2015, 3151 (3157, Rn. 91).
128 Kampert, in: Sydow (Hrsg.), 2020, § 48 BDSG, Rn. 17; Mysegades, NVwZ 2020, 852 (854).
129 Schwichtenberg, in: Kühling/Buchner (Hrsg.), DSGVO/BDSG, 3. Aufl., 2020, § 48 BDSG, Rn. 7.
130 Siehe Art. 8 II JI-RL.
131 Der Begriff der „optisch-elektronischen Einrichtung" umfasst auch Smart Cams; vgl. Grabenschröer/Reuter, in: Taeger/Gabel (Hrsg.), 3. Aufl., 2019, § 4 BDSG, Rn. 31 m. w. N.
132 Ebenso Frenzel, in: Paal/Pauly (Hrsg.), DSGVO/BDSG, 3. Aufl., 2021, § 4 BDSG, Rn. 14.
133 Die Systematik des BDSG steht diesem Rückgriff dagegen nicht im Wege. § 4 BDSG kann auch im Anwendungsbereich der JI-Richtlinie als Ermächtigungsgrundlage fungieren, Albers, in: Wolff/Brink (Hrsg.), § 48 BDSG, Rn. 10 (allerdings mit unionsrechtlichen Bedenken); Lang, in: Taeger/Gabel (Hrsg.), 3. Aufl., 2019, § 3, Rn. 14; Starnecker, in: Gola/Heckmann (Hrsg.), 13. Aufl., 2019, § 3, Rn. 2.
134 Dazu auch ausführlich Schindler, Biometrische Videoüberwachung, S. 407 ff.
135 Zur Frage, inwieweit § 100 h I Nr. 2 StPO auch die Aufzeichnung von Bildern als sonstige für Observationszwecke bestimmte technische Mittel iSd Vorschrift einstuft (verneinend), Günther, in: Knauer/Kudlich/Schneider (Hrsg.), MüKo StPO, 2014, § 100 h, Rn. 5; Schindler, Biometrische Videoüberwachung, S. 421.
136 Hegmann, in: Graf (Hrsg.), BeckOK StPO, 41. Ed. (Stand: 1.10.2021) § 100 h, Rn. 2; Günther, in: Knauer/Kudlich/Schneider (Hrsg.), § 100 h, Rn. 3. zu § 48 BDSG s. a. IV 1. a) bb).
137 Ausnahmsweise erlaubt § 100 h II 2 Nr. 1 StPO zwar auch Bildaufnahmen von sonstigen Personen, um den Aufenthaltsort eines Beschuldigten zu ermitteln. Die Legitimationswirkung der Vorschrift erstreckt sich jedoch auch in diesem Fall allein darauf, Bildaufnahmen *herzustellen*. Die Aufnahmen später im Wege eines automatisierten Abgleichs mit der Datenbank auszuwerten, richtet sich nach § 163 StPO i. V. m. § 48 BDSG. Das VG Hamburg erachtet § 48 BDSG als hinreichende Grundlage zur nachträglichen biometrischen Analyse im Rahmen konkreter Ermittlungen, VG Hamburg, 23.10.2019 – 17 K 203/19, BeckRS 2019, 40195, Rn. 77 ff. Die generalklauselartige Konstruktion der Vorschrift deckt den sehr grundrechtssensiblen Einsatz von Gesichtserkennungssoftware jedoch nicht. Siehe hierzu bereits IV. 1. a) bb).
138 Dafür müssen konkrete Anhaltspunkte vorliegen, die darauf hindeuten, dass der Betroffene zur Aufklärung beitragen kann, z. B. als Zeuge, Häfen, in: Graf (Hrsg.), BeckOK StPO, 41. Ed. (Stand: 1.10.2021), § 163 b, Rn. 14.
139 Kölbel, in: Knauer/Kudlich/Schneider (Hrsg.), MüKo StPO, 2016, § 163 b, Rn. 23; Schindler, Biometrische Videoüberwachung, S. 434.

Übereinstimmungsmuster überprüft. Allerdings genügt diese Erlaubnisnorm ebenso wenig den Anforderungen, die an die grundrechtliche Bestimmtheit einer Eingriffsgrundlage für Gesichtserkennung zu stellen sind.[140] Sie spricht insbesondere nicht von biometrischen Merkmalen als besonders sensiblen personenbezogenen Daten, sondern allgemein von „personenbezogene[n] Daten" (§ 98 c S. 1 StPO).

c) Zwischenergebnis

Echtzeit-Gesichtserkennungssoftware, wie im Falle des Pilotversuchs Südkreuz, dauerhaft und anlasslos einzusetzen, findet weder für präventive noch für repressive Maßnahmen eine tragfähige Eingriffsgrundlage, die der Sensibilität hinreichend Rechnung trägt, welche von der Kombination aus Videoaufzeichnung, automatisierter Analyse und Abgleich der biometrischen Daten mit einem Datenbankbestand ausgeht. Auch verfassungsrechtlich wäre eine zeitlich unbeschränkte, anlasslose Gesichtserkennung mit Blick auf ihre einschneidenden Grundrechtswirkungen kaum legitimierbar.[141]

2. Zweckspezifische, zeitlich begrenzte Gesichtserkennung (Fallkonstellation Sachsen)

Seit dem Sommer 2019 verwendet die Polizeidirektion Görlitz an bisher fünf[142] verschiedenen Standorten in der Altstadt Videosysteme, die nicht nur Kfz-Kennzeichen erfassen, sondern auch eine automatisierte Gesichtserkennung durchführen.[143] Die Kameras sind Teil eines 30 km breiten, entlang der tschechischen und polnischen Grenze eingerichteten Korridors zur Videoüberwachung, der schwere Grenzkriminalität bekämpfen soll.[144]

a) Normgehalt des § 59 SächsPVDG

Die sächsische Polizei stützt den Görlitzer *Smart-Camera*-Einsatz auf § 59 SächsPVDG.[145] Die Vorschrift ist deutschlandweit die erste Rechtsgrundlage, die (wenn auch etwas sybillinisch formuliert) nach dem erklärten Willen des Gesetzgebers[146] den Einsatz biometrischer Gesichtserkennungssoftware gefahrenabwehrrechtlich ermöglichen soll. Sie gestattet es den Behörden, – beschränkt auf bestimmte Räume und in zeitlichen Grenzen – im öffentlichen Verkehr personenbezogene Daten[147] in Gestalt von Bildaufzeichnungen zu erheben und diese automatisiert mit gespeicherten Daten eines bestimmten Personenkreises abzugleichen.

Das Sächsische Polizeivollzugsdienstgesetz lässt Gesichtserkennung nicht für *jede* polizeiliche Gefahr der Grenzkriminalität zu, sondern nur, um *schwere Straftaten* zu verhüten. Hierzu zählt das Gesetz u. a. Menschenhandel (§ 232 StGB), Bandendiebstahl (§ 244 I Nr. 2 StGB) sowie Raub (§ 249 StGB) – vgl. § 59 I 1 SächsPVDG i. V. m. § 100 a II Nr. 1 lit. j, l und n, Nr. 2 lit. b, Nr. 7 lit. a, b StPO. Die erhobenen Daten darf die Polizei überdies ausschließlich mit den Datensätzen solcher Personen automatisiert abgleichen, die wegen einschlägiger Straftaten zur polizeilichen Beobachtung ausgeschrieben sind (§ 59 II SächsPVDG). Die Voraussetzungen dafür bestimmen sich nach § 60 SächsPVDG. Diese Vorschrift erlaubt es, – sofern dies erforderlich ist – auch Kontaktpersonen Gesuchter zur Beobachtung auszuschreiben, bei denen „Tatsachen die Annahme rechtfertigen, dass sie in absehbarer Zeit eine zumindest der Art nach konkretisierte Straftat von erheblicher Bedeutung" (II Nr. 1) oder „in überschaubarer Zukunft eine terroristische Straftat" (II Nr. 2) begehen werden.

b) Vereinbarkeit mit höherrangigem Recht

Eingedenk der verfassungsrechtlichen Vorgaben benennt § 59 SächsPVDG einen *konkreten und objektiv bestimmbaren* Überwachungsgrund als Handlungsvoraussetzung. Dass die Norm die Kamera- und Gesichtserkennungssysteme in Sachsens Grenzgebieten tatsächlich in einer unions- und verfassungsrechtlich hinreichenden Weise deckt, ist damit jedoch nicht gesichert.

aa) Besondere Kategorien personenbezogener Daten

Blickt man auf die Art der Daten, die § 59 SächsPVDG zu verarbeiten gestattet, fällt auf, dass die Vorschrift lediglich auf „personenbezogene Daten" abhebt, nicht jedoch ausdrücklich jene *besonderen Kategorien* personenbezogener Daten, zu denen auch biometrische Daten gehören. Anders als bspw. § 4 I SächsDSUG[148] (vgl. § 2 Nr. 15 lit. c SächsDSUG[149]) differenziert das SächsPVDG weder unmittelbar in § 59 noch in den umliegenden Eingriffsgrundlagen zwischen den Arten der Daten, sondern verwendet pauschal und undifferenziert den Rechtsbegriff *personenbezogene Daten*.

Art. 10 JI-RL gibt eine Differenzierung zwischen der Verarbeitung *einfacher* personenbezogener Daten und *besonderer Kategorien* personenbezogener Daten in seinem Anwendungsbereich jedoch zwingend vor. Aus der unionsrechtlichen Vorgabe lässt sich e contrario schließen, dass eine mitgliedstaatliche Erlaubnisnorm ausdrücklich oder hinreichend klar auch die Verarbeitung besonderer Kategorien personenbezogener Daten gestatten muss. Sonst liefe das (alternative) Tatbestandsmerkmal in seiner Funktion ins Leere.

Immerhin die Gesetzesbegründung zu § 59 SächsPVDG spricht davon, dass die personenbezogenen Daten i. S. d. Abs. 2 auch biometrische Daten umfassen.[150] Das rechtfertigt – in Verbindung mit der Rationalität der Norm, der Gesichtserkennung den legitimatorischen Boden zu bereiten – noch eine (unionsrechtskonforme) Auslegung des grundsätzlich eindeutigen Wortlauts dahin, dass die Norm auch die besonderen Kategorien personenbezogener Daten (inkl. biometrischer Daten) umfasst.

140 Anders Schindler, Biometrische Videoüberwachung, S. 425 ff., 547; zur Frage, warum Gesichtserkennung sich nicht auf das Instrument der Rasterfahndung (§§ 98 a, 98 b StPO) stützen lässt, ders., aaO, insbesondere 422 ff. bzw. 425 ff.

141 Siehe dazu III. 2. b).

142 Die Stadt Görlitz plant derweil, die Videoüberwachung weiter auszubauen, vgl. Mehr „Argus"-Augen für grenznahe Städte zu Polen und Tschechien, mdr.de vom 15.4.2021; dpa, Polizei wertet Videoüberwachung in Görlitz als Erfolg, Süddeutsche Zeitung vom 7.2.2020.

143 Bender, Die unheimlichen Polizeikameras von Görlitz, faz.net vom 10.7.2020.

144 Vgl. § 59 I 2 SächsPVDG.

145 Er fand mit dem „Gesetz zur Neustrukturierung des Polizeirechtes des Freistaats Sachsen" in das SächsPVDG Eingang.

146 Vgl. LT-Drs. 6/14791, S. 186.

147 Bspw. Pkw-Kennzeichen und biometrische Daten.

148 Die Norm lässt eine Verarbeitung (neben anderen Voraussetzungen) auch nur dann zu, wenn dies in einer Rechtsvorschrift vorgesehen ist, die Verarbeitung der Wahrung lebenswichtiger Interessen dient oder sich auf Daten bezieht, die die betroffene Person öffentlich zugänglich gemacht hat. Von Letzterem ist nicht schon allein deswegen auszugehen, weil sich Personen im öffentlichen Raum bewegen. Da es sich bei der Aufklärung von Sach- und Vermögensdelikten auch nicht um lebenswichtige Interessen handelt, lässt das SächsDSUG eine Erhebung nur dann zu, wenn eine Rechtsvorschrift dies ausdrücklich vorgibt.

149 Das DSUG findet allerdings hier keine Anwendung, da das Polizeivollzugsdienstgesetz (PVDG) als Lex specialis vorrangig ist (§ 1 V SächsDSUG).

150 LT-Drs. 6/14791, S. 186.

bb) „Unbedingt erforderlich"

Als Erlaubnisnorm für biometrische Daten bietet § 59 SächsPVDG reichlich unions- und verfassungsrechtliche Angriffspunkte. Die Vorschrift benennt das Instrument der Gesichtserkennung zum einen nur unklar („durch den Einsatz technischer Mittel zur Anfertigung von Bildaufzeichnungen des Verkehrs auf öffentlichen Straßen" [§ 59 I 1 SächsPVDG]).[151] Damit die Verarbeitung der biometrischen Daten den sekundärrechtlichen Anforderungen des Art. 10 JI-RL genügt, muss sie zum anderen auch „unbedingt erforderlich" sein (vgl. auch § 48 BDSG): Sie muss sich auf das absolut Notwendige beschränken.[152] Dafür reicht es nicht aus, die polizeiliche Gefahrenabwehr sowie die Strafverfolgung lediglich zu *erleichtern*. Die Maßnahme muss vielmehr unentbehrlich sein, um den gesetzlich intendierten Zweck zu erreichen.[153] Die Messlatte der unionsrechtlichen Zulässigkeit liegt damit hoch. Für die verfassungsrechtliche Rechtfertigungslast gilt in der Sache nichts anderes, greift Gesichtserkennung doch tief in das informationelle Selbstbestimmungsrecht ein, indem sie biometrische Daten einer Vielzahl von Personen unabhängig von einem konkreten Tatverdacht erhebt, um einige wenige Personen zu identifizieren.

(1) Hinreichende örtliche Beschränkung?

Soll Gesichtserkennung „(unbedingt) erforderlich" sein, muss die Ermächtigungsnorm sicherstellen, dass die Überwachung nicht generell raumbezogen, sondern konkret ortsbezogen erfolgt.[154] Ein ganzes Netz von Straßenzügen und mehrere Kilometer ganzer Straßenabschnitte zu beobachten, schösse über das Gebot der (unbedingten) Erforderlichkeit und Angemessenheit hinaus.

§ 59 SächsPVDG beschränkt den räumlichen Einsatzradius für die Bildaufzeichnung und den Abgleich durch ein quantitatives und ein qualitatives Merkmal: Die Norm legitimiert Gesichtserkennung einerseits nur im grenznahen Bereich – bis zu 30 Kilometer ins Landesinnere von der Grenze zu Polen und Tschechien (§ 59 I 2 SächsPVDG; das sind allerdings immerhin ca. 50 % der Landesfläche Sachsens[155]). Die Datenerhebung darf andererseits auch innerhalb dieses Korridors ausschließlich an Orten erfolgen, die nachweislich eine herausgehobene Bedeutung für die grenzüberschreitende Kriminalität aufweisen. Diese muss sich aus polizeilich dokumentierten Tatsachen ergeben (§ 59 I 3 SächsPVDG).

§ 59 I 4 SächsPVDG bekennt sich damit zwar ausdrücklich dazu, dass eine flächendeckende Überwachung nicht erfolgen darf.[156] Wann „ein Straßenabschnitt" von „herausragender Bedeutung" für die grenzüberschreitende Kriminalität im Sinne des Abs. 1 S. 2 ist, skizziert die Norm aber nur schemenhaft: Sie beschränkt sich darauf, lediglich Gründe für diese besondere Eigenschaft zu benennen („[…], weil er regelmäßig als Begehungsort der Straftaten im Sinne des Satzes 1 oder für die Verbringung von Sach- oder Vermögenswerten aus diesen Straftaten genutzt wird.").

Dieses geringe Maß an Konkretisierung genügt rechtsstaatlichen Bestimmtheitsmaßstäben an die Weite des Überwachungsradius nicht. Die Eingriffsgrundlage klärt nämlich nicht hinreichend zweifelsfrei, ob die Polizeidienststelle als „Straßenabschnitt" im Sinne des Abs. 1 S. 2 auch mehrere Streckenkilometer ausweisen darf. Der Wortlaut der Norm lässt das durchaus zu. Überwachte Straßenabschnitte könnten sich dadurch auf ganze Regionen im Grenzgebiet erstrecken.[157] Die Überwachung nähme damit einen raumgreifenden Charakter an, der aufgrund seiner Unbestimmtheit und generellen Abschreckungswirkung verfassungsrechtlich nicht hinnehmbar ist.

(2) Hinreichende zeitliche Beschränkung?

Zum unions- und verfassungsrechtlichen Gebot der Erforderlichkeit gehört, dass aufgezeichnete Daten „nicht länger aufbewahrt werden [dürfen], als dies für den Zweck, zu dem sie verarbeitet werden, erforderlich ist" (ErwGr. 26 JI-RL).[158] Im Lichte dieser Anforderung unterwirft das Gesetz die Auswertung der Daten einer zweifachen zeitlichen Beschränkung: Das System darf grundsätzlich nur für einen Zeitraum von sechs Monaten zum Einsatz kommen. Nach Ablauf dieser Frist hat eine Prüfung zu erfolgen, ob die Anordnungsvoraussetzungen noch vorliegen (§ 59 III 2 SächsPVDG). Die Polizeibehörden müssen zudem eine Absicherung gegen eine dauerhafte Beobachtung der Bürger vornehmen: Sie sind verpflichtet, „[d]urch technisch-organisatorische Maßnahmen" sicherzustellen, dass die Kameras weder einzeln noch kumulativ als Dauerüberwachung der Streckenabschnitte wirken (§ 59 I 4 SächsPVDG). Welche Maßnahmen in praxi konkret vorzunehmen sind und wie sie sich technisch umsetzen lassen, lässt die Vorschrift hingegen offen. Als zusätzliche Verfahrenssicherung sieht sie immerhin Dokumentationspflichten vor: Für jeden Einsatz sind die einschlägigen Entscheidungsgrundlagen einschließlich der Lageerkenntnisse zu dokumentieren (§ 59 III 3, 4 SächsPVDG).[159] Ebenso muss der Präsident des LKA, der Präsident der jeweils zuständigen Polizeidirektion oder ein eigens für diese Aufgabe Beauftragter den Einsatz anordnen und „spätestens nach Ablauf von jeweils sechs Monaten […] prüfen, ob die Voraussetzungen für die Anordnung noch bestehen" (§ 59 III 2 SächsPVDG), damit keine Dauerüberwachung entstehen kann und die Anforderungen an den konkreten, objektiv bestimmbaren Grund über die gesamte Erhebungsdauer erfüllt sind.

Wenn die Polizei einen Ort wegen seiner herausragenden Bedeutung für die grenzüberschreitende Kriminalität via Gesichtserkennung überwacht, werden sich Begehungs- und Verwahrungsorte aber typischerweise schon viel früher verlagern: Potenziell Beschuldigte werden den offenen Einsatz der Technologie im Grenzgebiet schnell wahrnehmen und Alternativrouten über die Grenze wählen. Mittels örtlich flexibler Kontrollen kann die Polizei auf Routenverlagerungen fühlbar schneller sowie grundrechtsschonender reagieren und dadurch die große Mehrheit der von Gesichtserken-

151 In diesem Sinne auch Schindler, Biometrische Videoüberwachung, S. 544 f.
152 Petri GSZ 2018, 144 (146).
153 Vgl. auch Schwichtenberg, in: Kühling/Buchner (Hrsg.), § 48 BDSG, Rn. 3.
154 BVerfGE 150, 244 (289) = NJW 2019, 827 (836, Rn. 115).
155 Bender (Fn. 143).
156 Siehe auch die Gesetzesbegründung (wenn auch zur ähnlichen Regelung der automatischen Kennzeichenerfassung in § 58 II 2 SächsPVDG): LT-Drs. 6/14791, S. 184 sowie BVerfGE 150, 244 (300, Rn. 149).
157 Begründung der abstrakten Normenkontrolle von Abgeordneten des Sächsischen Landtags gegen das SächsPVDG vom 1. August 2018, abrufbar unter https://www.gruene-fraktion-sachsen.de/wp-content/uploads/2019/08/201908-Normenkontrollklage-Polizeigesetz.pdf, S. 52.
158 ErwGr. 37 JI-RL zählt entsprechende Referenzfälle auf. Zu den geeigneten Garantien für die Rechte und Freiheiten der betroffenen Person zählt er bspw. die rechtliche Verpflichtung, Daten nur in Verbindung mit anderen Daten über die betroffene natürliche Person zu erheben, die erhobenen Daten hinreichend zu sichern, den Zugang der Mitarbeiter der zuständigen Behörde zu den Daten strenger zu regeln und die Übermittlung dieser Daten zu verbieten.
159 Vgl. auch BVerfGE 133, 277 (370); 141, 220 (284 ff.); 150, 244 (303, Rn. 157).

nungssystemen Betroffenen, deren Abgleich zu Nichttreffern führt, verschonen.

Regelmäßig ist es daher geboten, die Anordnung bereits vor Ablauf der Sechsmonatsfrist zu überprüfen. So deutet es auch der Gesetzeswortlaut („spätestens") im Grundsatz an. Mit Blick auf die hohe Eingriffsintensität der Gesichtserkennung bewegt sich eine sechsmonatige gesetzliche Regelfrist jedoch an der Grenze des verfassungsrechtlich Vertretbaren.[160]

Dass die Polizei die Daten nicht nur aufzeichnet und mit einer Gesichtserkennungssoftware analysiert, sondern – auch bei sog. Nichttreffern – über (mindestens) 96 Stunden speichert (§ 59 I 2 SächsPVDG), greift zusätzlich tief in das Grundrecht auf informationelle Selbstbestimmung ein.[161] Die mit dieser Form der Vorratsdatenhaltung einhergehenden Abschreckungseffekte können (samt des potenziellen Missbrauchsrisikos) eine schleichende Selbsteinschränkung unbescholtener Bürger nach sich ziehen. Das erhöht die Rechtfertigungslast.

Die Gesetzesbegründung rechtfertigt die Frist damit, dass 96 Stunden erforderlich seien, „um ausreichend Zeit zur Bestimmung des in den Abgleich einzubeziehenden Personenkreises und Durchführung und Auswertung/Verifizierung des Abgleichs einzuräumen."[162] Technisch ist eine solche lange Speicherdauer aber nicht erforderlich. Diejenigen Personen, die das System erfassen soll, muss die Polizei ohnedies im Voraus bestimmen und in die Datenbank aufnehmen – es gleicht dann lediglich die Gesichter (und Kennzeichen) aus der Überwachungsmaßnahme mit der Datenbank ab. Eine Vorratsdatenhaltung ist allenfalls erforderlich, um das System stichprobenartig zu überprüfen (etwa um sog. False Negatives zu identifizieren). Grundrechtlich ist eine solche Speicherlänge bei Abwägung der kollidierenden Schutzgüter aber regelmäßig nicht mehr rechtfertigbar. Vielmehr ist im Nicht-Trefferfall eine sofortige Löschung geboten, um den Grundrechtseingriff für unbeteiligte und unverdächtige Personen auf das technisch mögliche Minimum zu begrenzen und diejenigen Personen, welche die Polizei erfassen will, im Voraus zu bestimmen und in die Datenbank aufzunehmen. Dies gilt insbesondere für Kontaktpersonen potenzieller „Gefährder", die zur Fahndung ausgeschrieben sind. Ihre Daten löscht das System nicht automatisch (vgl. § 60 II Nr. 3 i. V. m. Nr. 1 SächsPVDG). Da die Einstufung als „Gefährder" oftmals im Vorfeld einer Straftatbegehung erfolgt, speichern die Behörden in der Datenbank somit ggf. auch Daten unbescholtener Personen, die lediglich Kontakt zu einem – zumindest bisher – nicht straffällig gewordenen Bürger hatten.

cc) Verfahrensrechtliche Schutzmechanismen für die Rechte und Freiheiten Betroffener

§ 59 SächsPVDG garantiert durch Aufsichtsmechanismen und Dokumentationspflichten zwar ein Mindestmaß aufsichtsrechtlicher Kontrolle und Transparenz: Die Staatsregierung hat die Erforderlichkeit, die praktische Anwendung und die Auswirkungen der Gesichtserkennung zu prüfen und dem Landtag zu berichten (§ 60 IV SächsPVDG). Allerdings stellt das Sächsische Polizeirecht keine sonstige externe Kontrolle sicher, die für eine kritische Distanz bürgt. Der Präsident des LKA oder einer Polizeidirektion bzw. eine von ihm beauftragte Person gewährleistet – anders als bspw. ein Richter oder der Landesdatenschutzbeauftragte – gerade keine *externe* Kontrolle. Angesichts der weiten Streubreite und der hohen Eingriffsintensität der Maßnahme implementiert eine interne Kontrolle daher keinen ausreichenden Schutzmechanismus für die Betroffenen. Insbesondere ein Richtervorbehalt eröffnete aufgrund der sachlichen und persönlichen Unabhängigkeit des Richters (Art. 97 GG) ein sachadäquates Instrument, um ein wirksames präventiv wirkendes, verfahrensrechtliches Gegengewicht des Grundrechtsschutzes gegen die Versuchung zu setzen, von den technischen Möglichkeiten extensiv Gebrauch zu machen.[163]

Bislang lässt es das Gesetz auch an Regelungen dazu vermissen, wie Fehlerrisiken der Datenbank, z. B. mit Blick auf Diskriminierungen etc., rechtlich einzuhegen sind. Angesichts des nicht unbeträchtlichen, grundrechtlich sensiblen Fehlerrisikos von Gesichtserkennungssoftware wären verfahrensrechtliche Vorkehrungen angezeigt, die das Risiko auf ein vertretbares Maß reduzieren.

dd) Zwischenergebnis

Der sächsische Landesgesetzgeber hat für den Einsatz intelligenter Videoüberwachung, die auch auf Gesichtserkennungssoftware setzt, für sachgebietsspezifische, zeitlich begrenzte Zwecke eine spezielle Eingriffsgrundlage geschaffen. In ihrer konkreten Ausgestaltung genügt die Norm aber nicht den unions- und verfassungsrechtlichen Anforderungen, die es zu erfüllen gilt, um ihren tief gehenden Eingriff in die Rechtspositionen Betroffener zu rechtfertigen.

3. Anlassbezogene Gesichtserkennung zur Einlasskontrolle gefährdeter Orte (Fallkonstellation Großveranstaltung/Fußballstadion)

Nicht nur an infrastrukturellen Knotenpunkten, wie Grenzen oder Bahnhöfen, kann Gesichtserkennung substanzielle Effizienz- und Sicherheitsvorteile generieren. Auch bei Zugangskontrollen zu besonders sicherheitsrelevanten Bereichen, etwa zu Großveranstaltungen oder behördlich genutzten Gebäuden, können *Smart Cams* kraft ihrer Auswertungsschnelligkeit einzelne Gefährder gezielt aus einer Menschenmenge herausfiltern. Sie eignen sich auch dazu, Personenzählungen und Personendichtemessungen vorzunehmen, die es den Sicherheitskräften vor Ort ermöglichen, ungewöhnliche Bewegungen zu lokalisieren und ggf. einzugreifen. Manche Systeme arbeiten mit Wärmeerkennung,[164] andere dagegen erfassen die biometrischen Merkmale der Personen.

a) Mögliche Einsatzszenarien

Erste Erfahrungen bei der Überwachung großer Menschenmengen mit *Smart Cams* hat die Polizei in South Wales bereits im Juni 2017 gesammelt. Sie setzte automatisierte Gesichtserkennung im Umfeld von Fußballspielen ein, um Live-Bilder aus den Überwachungskameras mit den Bildern von Straftätern in der polizeieigenen Datenbank abzugleichen.[165] Einer nicht unerheblichen Fehlerquote falsch-positiver Treffer[166] zum Trotz bewertete die Polizei das Projekt als

160 Ähnlich auch die Begründung der abstrakten Normenkontrolle von Abgeordneten des Sächsischen Landtags gegen das SächsPVDG vom 1. August 2018 (Fn. 157), S. 53.
161 Vgl. III. 1. a).
162 LT-Drs. 6/14791, S. 186.
163 In diesem Sinne sieht Art. 5 III des Vorschlags für ein Gesetz über Künstliche Intelligenz die vorherige Genehmigung des Einsatzes von Echtzeit-Gesichtserkennungssystemen durch eine Justizbehörde oder unabhängige Verwaltungsbehörde vor. Ebenso aus nationaler Perspektive Schindler, Biometrische Videoüberwachung, S. 611.
164 In das Recht auf informationelle Selbstbestimmung greift die Maßnahme erst dann ein, wenn die Möglichkeit besteht, Menschen zu individualisieren.
165 Reuter, Gericht erklärt automatisierte Gesichtserkennung in Südwales für illegal, netzpolitik.org vom 12.8.2020.
166 Von den 2470 Trefferalarmen bei 170.000 Teilnehmern einer Veranstaltung waren 2297 falsche Treffer. Die Fehlerquote lag damit bei 92 %.

Erfolg.[167] Der britische High Court of England and Wales hatte das Pilotprojekt zunächst für zulässig erklärt.[168] Das Berufungsgericht hat diese Entscheidung demgegenüber teilweise aufgehoben.[169] Der Rechtsrahmen habe den Einsatz der Gesichtserkennung nicht hinreichend eingegrenzt und damit den Polizeibeamten einen zu weitreichenden Ermessensspielraum zugestanden.[170] Überdies habe die Polizei nicht untersucht, ob das Gesichtserkennungssystem geschlechtsspezifisch oder rassistisch diskriminiere.

Hierzulande liebäugeln die Sicherheitsbehörden ebenfalls damit, automatisierte Gesichtserkennung bei Großveranstaltungen zu nutzen. Die Polizei Hamburg hat bspw. bereits in Aussicht gestellt, Echtzeit-Systeme bei Großveranstaltungen, wie dem traditionell emotionsgeladenem Fußballderby zwischen dem HSV und dem FC St. Pauli, einsetzen zu wollen.[171]

b) Rechtsgrundlagen

Bei Großveranstaltungen kommt Gesichtserkennung qua natura anlassbezogen zum Einsatz: Die Dauer sowie das Ausmaß der Maßnahme sind limitiert und stehen bereits im Vorhinein fest. Das begrenzt das Risiko einer grundrechtlich besonders rechtfertigungsbedürftigen Datenvorratshaltung.

Allerdings setzt auch der anlassbezogene Einsatz der Gesichtserkennungstechnologie eine den verfassungsrechtlichen Anforderungen des Bestimmtheitsgrundsatzes sowie des Prinzips der Verhältnismäßigkeit genügende Eingriffsgrundlage voraus, entfaltet die Überwachung doch eine erhebliche Breitenwirkung, die mit Eingriffen in sehr sensible Rechtsgüter auch unbescholtener Personen einhergeht und damit hohe Streuschäden in Kauf nimmt. Ihre *Chilling effects* können mitunter viele Personen unbeabsichtigt von einem Veranstaltungsbesuch abschrecken, sodass diese ihre grundrechtlich verbürgten Freiheiten nicht mehr wahrnehmen. Dazu tragen die Undurchschaubarkeit des technischen Systems sowie das potenzielle Missbrauchsrisiko und die Fehlerquote der Gesichtserkennungsmaßnahmen nachhaltig bei.

Die Landes- und Bundesgesetze halten keine spezialgesetzlichen Verarbeitungsgrundlagen vor, welche die grundrechtlichen Eingriffswirkungen der Gesichtserkennung bei Einlasskontrollen abdecken. § 4 I Nr. 1 BDSG gestattet zwar die Videoüberwachung öffentlich zugänglicher Räume, um Aufgaben öffentlicher Stellen zu erfüllen. Gesichtserkennung legitimiert die Vorschrift aber nicht. Den Anforderungen an eine hinreichend bestimmte Rechtsgrundlage, welche die Zwecke, die Art und den Umfang des Einsatzes automatisierter Gesichtserkennung konkretisiert, genügt die Norm nicht.[172]

Auch auf die Generalklauseln der Polizei- und Datenschutzgesetze (z. B. § 14 I BPolG, § 9 I POG RLP, § 17 I ASOG Bln) lassen sich Systeme automatisierter Gesichtserkennung zum Zwecke der Kontrolle von Großveranstaltungen nicht stützen. Die Tatbestände sind (ebenso wie §§ 48, 4 I Nr. 1 und Nr. 2 BDSG) nicht hinreichend spezifisch und bestimmt genug, um die Schwere der Grundrechtseingriffe zu rechtfertigen, die Gesichtserkennung auslöst.

Wie für die anderen Anwendungsszenarien, in denen die Polizei automatisierte Gesichtserkennung zur Gefahrenabwehr einsetzt, besteht im deutschen Recht mithin auch bei der Einlasskontrolle zu Großveranstaltungen oder sonstigen gefährdeten Orten de lege lata keine Eingriffsgrundlage, die den Einsatz biometrischer Erkennungssysteme legitimiert.

V. Fazit, Anforderungen an eine Eingriffsgrundlage de lege ferenda und Ausblick

Gesichtserkennung wandelt auf einem schmalen Grat zwischen der staatlichen Schutzpflicht für die Sicherheit und der Gefahr unangemessener Einschüchterung auch unbescholtener Bürger. Ihr Einsatz zum Zwecke der Strafverfolgung und Gefahrenabwehr birgt einerseits besondere Schlagkraft. Sie kann andererseits aber auch den Beginn eines Zeitalters ubiquitärer Massenüberwachung einläuten – und dadurch unser historisch gewachsenes Selbstverständnis von Privatsphäre sowie das gesellschaftliche Miteinander fundamental umwälzen. Die Technologie vollzieht damit einen grundlegenden Paradigmenwechsel in der Sicherheitspolitik.

Während die Verfassung und Art. 10 JI-RL für den anlasslosen oder flächendeckenden Einsatz biometrischer Gesichtserkennung keinen Raum lassen,[173] darf ihr Einsatz anlassbezogen und örtlich sowie zeitlich begrenzt in zulässiger Weise erfolgen. Der Gesetzgeber ist dafür aber auf eine nach Anlass, Zweck und Grenzen des Einsatzes hinreichend bestimmte Ermächtigungsnorm angewiesen. Um dem verfassungs- und unionsrechtlich[174] radizierten rechtsstaatlichen Verhältnismäßigkeitsprinzip sowie dem Bestimmtheitsgebot zu genügen, sind verfahrensrechtliche Konkretisierungen der Voraussetzungen, Modalitäten und Grenzen der automatisierten Gesichtserkennung essenziell. Flankierend sind ferner korrespondierende Transparenzvorkehrungen und Rechtsschutzmöglichkeiten des Einzelnen geboten.

1. Verhältnismäßigkeit

Dass Gesichtserkennung die Effizienz polizeilicher Arbeit verbessert sowie Abschreckungseffekte bei Gefährdern erzielen kann, legitimiert ihren Einsatz noch nicht. Sie ist stets Ultima Ratio – nicht zuletzt, weil sie auch Nichtstörer in Anspruch nimmt.

Auf den ersten Blick scheinen sog. *Super Recognizer*, wie sie die Bayerische Polizei bereits beim Oktoberfest in München, die baden-württembergische Polizei bei der Aufklärung sommerlicher Ausschreitungen in Stuttgart im Jahre 2020[175] oder die Frankfurter Polizei bei Protesten im Dan-

167 Rötzer, Gesichtserkennung von Menschenmassen mit einer Fehlerrate von 92 Prozent, heise.de vom 6.5.2018; siehe auch Press Association, Welsh police wrongly identify thousands as potential criminals, The Guardian online vom 5.5.2018.

168 R (Bridges) v CCSWP and SSHD, [2019] EWHC 2341. Die dortige Sachverhaltsdarstellung eröffnet zudem einen sehr instruktiven Einblick in die Details der polizeilichen Gesichtserkennungspraxis in Süd-Wales (Rn. 23 ff.). In den Augen des Gerichts verletzt die Software nicht die Rechte des Klägers: Sie stehe auf hinreichender rechtlicher Grundlage (Rn. 96) und sei mit dem Data Protection Act 2018, der die DSGVO ergänzt und die JI-RL umsetzt, in Einklang (Rn. 132 ff., 148). Auch Art. 8 EMRK sahen die Richter nicht verletzt (Rn. 62).

169 R (Bridges) v CCSWP and SSHD, [2020] EWCA Civ 1058. Es sei z. B. nicht hinreichend klar geregelt, welche Personen für die Watchlist gewählt werden können (Rn. 54 ff.).

170 R (Bridges) v CCSWP and SSHD, [2020] EWCA Civ 1058.

171 Monroy, Soko „Schwarzer Block“: Hamburger Datenschutzbeauftragter hält Gesichtserkennung für rechtswidrig, netzpolitik.org vom 15.8. 2018.

172 S. dazu auch bereits IV. 1. a) cc); § 4 I Nr. 2 BDSG gestattet Videoüberwachung zwar auch, um das Hausrecht wahrzunehmen. Die Polizei kann sich jedoch nicht auf das Hausrecht berufen, wenn sie außerhalb ihrer Gebäude für Dritte Aufgaben der öffentlichen Sicherheit wahrnimmt. Es steht in diesem Fall nur dem Veranstalter des Großereignisses zu, nicht aber der Polizei.

173 So auch Kulick NVwZ 2020, 1622 (1626); aA Schindler, Biometrische Videoüberwachung, S. 624.

174 Gesichtserkennung muss insbesondere „unbedingt erforderlich“ sein, um die polizeiliche Aufgabe zu erfüllen (vgl. Art. 10 JI-RL).

175 Baden-Württemberg, Polizei etabliert „Super-Recogniser“, https://www.baden-wuerttemberg.de/de/service/presse/pressemitteilung/pid/polizei-etabliert-super-recogniser-1/ (3.11.2021).

nenröder Forst eingesetzt hat, das grundrechtsschonendere Mittel.[176] Super Recognizer sind Personen, die sich außergewöhnlich gut Gesichter einprägen und diese – auch Jahre nach einer flüchtigen Begegnung – wiedererkennen können.[177] Ca. 1 bis 2 % der Bevölkerung verfügen über diese außergewöhnliche Fähigkeit. Sie können Personen auf Bildmaterial identifizieren,[178] selbst wenn dieses unscharf, verwackelt oder unterbelichtet ist. Allerdings erreichen zum einen auch solche Helfer ihre natürlichen Grenzen. Tausende von Gesichtern können sich auch Super Recognizer nicht ohne Weiteres merken. Ebenso wie Maschinen unterlaufen ihnen Erkennungsfehler. Es ist zum anderen nicht generell weniger invasiv und grundrechtsschonender, Menschen bei der Identifikation von Personen einzusetzen. Gesichtserkennungstechnologie ist dem Gesetzgeber daher nicht von vornherein unter dem Gesichtspunkt der Verhältnismäßigkeit verwehrt.

Mit Blick auf die hohe Beeinträchtigungswirkung, die von automatisierter Gesichtserkennung ausgeht, rechtfertigt nicht jeder, sondern nur ein besonders schwerwiegender Zweck ihren Einsatz. Die zulässigen Einsatzziele sind in *sachlicher* Hinsicht darauf zu beschränken, Schwerkriminalität zu verhindern bzw. zu verfolgen oder erhebliche Gefahren für überragend wichtige Rechtsgüter abzuwehren. Dies begrenzt den Adressatenkreis der Gesuchten auf Personen, bei denen konkrete Hinweise auf solche schweren Straftaten greifen oder die bereits entsprechender Straftaten verdächtig sind. Um den Begriff „Schwerkriminalität" zu kategorisieren, liefert der Straftatenkatalog des § 100 a II StPO eine taugliche Blaupause.

Räumlich ist der Einsatz auf Orte zu limitieren, die besonders gefährdet sind. Dafür sind konkrete Anhaltspunkte erforderlich. Anderenfalls wäre einem flächendeckenden und damit über das Maß des unbedingt Erforderlichen hinausschießenden Einsatz der Boden bereitet.[179]

Ein verhältnismäßiger Einsatz automatisierter Gesichtserkennung ist nicht zuletzt strengen Anforderungen an die Datenminimierung[180] und Datenauswertung unterworfen. Abgleiche und Aufzeichnungen sind auf das Notwendigste zu begrenzen. Dazu gehören insbesondere technische und organisatorische Schutzmechanismen, die sicherstellen, dass die Polizei nur solche Daten erhebt, die für den Auswertungszweck zwingend erforderlich sind. Bei der Videoüberwachung einer Versammlung sollte bspw. eine Kamera, die lediglich Übersichtsaufnahmen aufzeichnen soll, erkannte Gesichter im Grundsatz schon bei der Datenerhebung unkenntlich machen.[181] Datenintegrität verlangt, dass die gespeicherten Gesichtsdaten vollständig, hinreichend genau[182] und konsistent sind. Öffentliche Stellen, die Gesichtserkennung einsetzen, müssen mit Blick auf das Fehlerrisiko der Software auch sicherstellen, dass die Daten, die sie verwenden, richtig sind, sie also insbesondere Bilder den richtigen Personen zuordnen.[183] Die Trainingsdaten müssen repräsentativ sein und Diskriminierungen vermeiden sowie rechtmäßig erhoben sein.[184] Für die Prävention und Repression von Schwerkriminalität sind als – in der gesetzlichen Eingriffsgrundlage zu benennende – Referenzdatenbanken nur eng umgrenzte polizeiliche Datenbanken zuzulassen, die für den jeweiligen Fahndungszweck relevant sind.[185] Die Eingriffsgrundlage muss auch hohe Anforderungen an die (sonstige) Datensicherheit gewährleisten.[186] Denn jedes Datenleck hätte für Betroffene verheerende Auswirkungen.[187] Manipulationen und Verfälschungen gilt es, mit Hilfe technischer Sicherungen wirksam einen Riegel vorzuschieben.

Auch die Speicherdauer ist auf das unbedingt Erforderliche zu begrenzen (Grundsatz der Speicherbegrenzung; Art. 4 I lit. e, Art. 5 JI-RL): Sobald die Polizei ein Ermittlungsverfahren gegen eine Person eröffnet, sammelt sie die Eckdaten des Sachverhalts samt personenbezogener Daten zum Beschuldigten in einer Datenbank. Es muss sichergestellt sein, dass die Daten nicht länger gespeichert werden, wenn sich der Anfangsverdacht nicht zu einem hinreichenden Tatverdacht verdichtet. Bei Nichttreffern sind die Daten Betroffener unmittelbar zu löschen. Allein die Tatsache, dass die Behörden irgendwann einmal gegen eine Person ermittelt haben, kann sonst nachhaltige grundrechtliche Konsequenzen zeitigen – etwa bei einer Zugangskontrolle. Betroffene müssen zumindest die Möglichkeit haben, rechtlich gegen eine Speicherung ihrer Daten über die Dauer des Ermittlungsverfahrens hinaus vorzugehen. Dazu müssen sie um die Tatsache der Datenaufbewahrung wissen. Entsprechende Informationsmaßnahmen sind insoweit zu treffen. Die Verarbeitungsgrundlage sollte auch sicherstellen, dass die Daten nicht für andere Zwecke als den Abgleich mit dem Fahndungsbestand zum Einsatz kommen, sondern die Zweckbindung gewahrt bleibt.[188]

2. Verfahrensrechtliche Anforderungen, insbesondere Transparenz

Beim Einsatz automatisierter Gesichtserkennung ist im Grundsatz Transparenz für jeden Passanten zu gewährleisten. Deutlich sichtbare Hinweise auf den Einsatz der *Smart Cam* bzw. der Gesichtserkennungstechnik sowie auf den Zweck der Maßnahme müssen jeden Passanten erkennen lassen, welche biometrischen Merkmale das System erfasst und mit welchen Datenbanken es einen Abgleich vornimmt. Um die notwendige Transparenz herzustellen, ist es geboten, korrespondierende Auskunftsansprüche und angemessene Rechtsschutzmöglichkeiten in der Norm zu verankern (Art. 12 ff. JI-RL). Ausnahmen vom Transparenzgebot sind

176 Bernstein, Polizisten, besser als eine Gesichtserkennungs-Software, SZ online vom 28.8.2018; Iskandar, Frankfurter Polizei setzt „Super Recogniser" ein, faz.net vom 11.2.2021. Siehe zum Einsatz von Super Recognizern bei der Bundespolizei auch die Antwort der Bundesregierung auf die Kleine Anfrage der FDP-Fraktion vom 22.6.2021, BT-Drs. 19/30906.

177 Bspw. identifizierte der Polizist Andy Pope zwischen 2012 und 2017 insgesamt 1.000 Verdächtige, Moshakis, Super recognisers: the people who never forget a face, The Guardian online vom 11.11.2018. Zu Super Recognizern siehe auch Schindler, Biometrische Videoüberwachung, S. 120 f.

178 Die Super Recognizer der London Metropolitan Police gleichen zB CCTV-Aufnahmen mit Fotos von Tatverdächtigen ab oder halten beim Streifengang Ausschau nach ihnen, Moshakis (Fn. 177).

179 BVerfGE 120, 378 (431).

180 Den Grundsatz der Datenminimierung normiert die JI-RL zwar nicht ausdrücklich, sehr wohl aber Art. 5 I lit. c DSGVO; vgl. auch Albrecht/Jotzo, Das neue Datenschutzrecht der EU, 2017, Teil 2: Grundsätze der DSGVO, D. Datensparsamkeit und Speicherbegrenzung, Rn. 6 ff.

181 Dieser Vorgang wäre auch nicht als erlaubnispflichtige Erhebung biometrischer Daten zu qualifizieren, da diese dem Zweck nach gerade nicht anonymisiert werden sollen, vgl. Schwenke NJW 2018, 823 (825).

182 Dass manchmal selbst herkömmliche Fahndungsfotos auf falschen Bildern beruhen können, demonstriert das Urteil des LG Osnabrück vom 7.7.2021 – 4 O 3406/19, ZD 2021, 218 f.

183 Ein Recht auf Berichtigung oder Löschung ergibt sich für Betroffene aus Art. 16 JI-Rl.

184 Siehe auch Art. 10 des Entwurfs der Kommission für die Regulierung Künstliche Intelligenz.

185 Vgl. auch BVerfGE 150, 244 (287, Rn. 108 ff.).

186 Vgl. Art. 29 JI-RL sowie Art. 15 IV des Entwurfs der Kommission für die Regulierung Künstliche Intelligenz. Dazu auch V. 4.

187 Siehe zB Goodman, Future Crime, 2015, S. 345 ff.; Hao/O'Neill, The hack that could make face recognition think someone else is you, MIT Technology Review vom 5.8.2020.

188 BVerfGE 150, 244 (304, Rn. 162 ff.).

nur für besondere Fälle der Aufklärung schwerer Straftaten rechtfertigbar.

3. Vorschlag der Kommission für eine Verordnung über Künstliche Intelligenz

Bis der nationale Gesetzgeber eine verfassungskonforme Regelung für Gesichtserkennungssysteme erlassen hat, wird womöglich bereits das „*Gesetz über Künstliche Intelligenz*“ (KIG)[189] die Weichen für Gesichtserkennung unionsweit einheitlich neu gestellt haben.

Der Entwurf der Kommission will sog. *biometrische Echtzeit-Fernidentifizierungssysteme*,[190] die die Gesichtserkennung in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken durchführen, grundsätzlich verbieten (Art. 5 I lit. d KIG-E). Zulässig sollen sie nur ausnahmsweise sein, um Opfer einer Straftat (insbesondere vermisste Kinder) ausfindig zu machen, Lebensgefahr oder Gesundheitsgefahren natürlicher Personen oder einen terroristischen Angriff abzuwenden oder spezifische Straftaten aufzuklären (Art. 5 I lit. d (i)-(iii) KIG-E).[191] Ihr Einsatz muss dann aber erforderlich und verhältnismäßig sein, insbesondere zeitlich, geografisch und personell begrenzt (Art. 5 II KIG-E). Eine Justizbehörde oder unabhängige Verwaltungsbehörde muss den Einsatz[192] gestatten (Art. 5 III KIG-E). Ergänzend sind – entsprechend dem bisherigen Grundmodell datenschutzrechtlicher Mechanismen – Schutzmaßnahmen zu treffen, welche die Rechte Betroffener hinreichend sichern (Art. 5 II KIG-E).

Die *übrigen Einsatzszenarien biometrischer Gesichtserkennung* – insbesondere eine Ex-post-Gesichtserkennung – lässt der Entwurf des KIG demgegenüber zu. Als KI-Systeme mit „hohem Risiko" (Art. 6 II i. V. m. Annex III Nr. 1 KIG-E) müssen sie aber eine ganze Reihe von Anforderungen, u. a. an ihre Genauigkeit, Belastbarkeit und IT-Sicherheit sowie an die Trainings-, Validierungs- und Testdatensätze erfüllen (Art. 8 ff. KIG-E). Außerdem haben sie Transparenz zu gewährleisten und menschliche Aufsicht[193] zu ermöglichen (Art. 13 und 14 KIG-E). Zulässig sind solche Hochrisiko-KI-Systeme auch nur dann, wenn sie eine Konformitätsbewertung durch eine unabhängige Stelle durchlaufen haben, welche die Übereinstimmung des Systems mit dem geltenden Recht validiert (Art. 19 I i. V. m. Art. 43 KIG-E).[194]

Das Europäische Parlament hält demgegenüber eine deutlich strengere Gangart gegenüber Gesichtserkennung für angezeigt: Es will die Technologie im öffentlichen Raum gänzlich untersagen.[195] Im Laufe des Gesetzgebungsverfahrens wird der Entwurf im Zweifel noch zahlreiche Änderungen erfahren. Die Union wird insbesondere unter Beweis stellen müssen, dass sie überhaupt auf eine hinreichende Kompetenz für detaillierte, unmittelbar geltende Regelungen zum polizeilichen Einsatz Künstlicher Intelligenz zurückgreifen kann. Denn mit ihrem Entwurf gibt sie unmittelbar Schlüsselelemente der nationalen Sicherheitsstrategie im Bereich der Künstlichen Intelligenz verbindlich vor. Die Nationale Sicherheit (insbesondere Störungen der öffentlichen Sicherheit, die nationale Bedeutung haben und die Sicherheit des Staates selbst betreffen) gehört zur Kernkompetenz der Mitgliedstaaten, welche die Eigenstaatlichkeit konstituiert. Das erkennen die unionsrechtlichen Verträge auch ausdrücklich an (Art. 4 II 2 und 3 EUV). Im Bereich des Polizeirechts verfügt die Union daher grundsätzlich nur über die Kompetenz, die grenzüberschreitende polizeiliche Zusammenarbeit zu regeln (Art. 87 ff. AEUV). Weder die Kompetenz für den Binnenmarkt (Art. 116 AEUV) noch die Datenschutz-Kompetenz der Union (Art. 16 AEUV) ändern daran etwas.[196] Diese stehen unter dem Vorbehalt, die Kompetenz der Mitgliedstaaten für die nationale Sicherheit nicht anzutasten. Dem Subsidiaritätsgrundsatz der Verträge entspricht es, den Mitgliedstaaten bei der Gestaltung ihrer KI-Instrumente als Teil ihrer nationalen Sicherheitspolitik Regelungsspielräume zuzugestehen. Tut die Union dies – wie der gegenwärtige Entwurf der Kommission – nicht, überschreitet sie ihren Kompetenzradius.

4. Rechtspolitische Herausforderungen

Das Bestreben der Sicherheitsbehörden, Gesichtserkennungsmethoden als gesetzlich anerkannte Werkzeuge in ihrem Handlungsrepertoire zu verankern, stößt immer stärker auf zivilgesellschaftlichen Widerstand[197] und ruft grundlegende ethische Fragen[198] auf den Plan, die das Recht allein nicht zu beantworten vermag. Denn Gesichtserkennung verändert unmittelbar die Architektur des öffentlichen Raums. Sie betrifft letztlich alle, die sich dort bewegen. Auch der unbescholtene Bürger vermag sich ihr nicht zu entziehen. Freiheit und Sicherheit stehen dabei einander als Gegenpole mitunter unversöhnlich gegenüber. Die Gesellschaft muss sich entscheiden. Handlungsleitend sollte dabei die Erkenntnis sein, dass Demokratien von der Verfügbarkeit unüberwachter öffentlicher Räume leben – dabei sollte es auch bleiben. ■

189 Vorschlag für eine Verordnung des Europäischen Parlaments und Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung bestimmter Rechtsakte der Union vom 21.4.2021, COM(2021) 206 final, 2021/0106(COD).

190 Siehe Art. 3 Nr. 37 und 38 des Vorschlags eines Gesetzes über Künstliche Intelligenz.

191 Als Leges speciales genießen die Vorschriften gegenüber der JI-RL Vorrang, vgl. Veale/Zuiderveen Borgesius, Demystifying the Draft EU Artificial Intelligence Act, 6.7.2021, S. 7.

192 Ob sich die Genehmigung auf den allgemeinen Ort bzw. Zweck oder auf konkrete Zwecke beziehen muss, ist unklar; vgl. Veale/Zuiderveen Borgesius, Demystifying the Draft EU Artificial Intelligence Act, 6.7.2021, S. 8.

193 Die Anbieter müssen Gesichtserkennungssysteme so gestalten, dass zwei natürliche Personen die Identifizierung bestätigen (Art. 14 V KIG-E); dies ist zu protokollieren (Art. 12 IV lit. d KIG-E). Wer die menschliche Aufsicht übernimmt, soll die „erforderliche Kompetenz, Ausbildung und Befugnis“ mitbringen (ErwGr. 48 KIG-E). Die Behörden, die Ex-post-Gesichtserkennung einsetzen, können die Organisation der Maßnahmen menschlicher Aufsicht weitestgehend selbst bestimmen (vgl. auch Art. 29 II KIG-E).

194 Kritisch zur Konformitätsbewertung und zur Rolle der Europäischen Komitees für Normung: Veale/Zuiderveen Borgesius, Demystifying the Draft EU Artificial Intelligence Act, 6.7.2021, S. 13 ff.

195 Entschließung des Europäischen Parlaments vom 6. Oktober 2021 zu dem Thema: Künstliche Intelligenz im Strafrecht und ihre Verwendung durch die Polizei und Justizbehörden in Strafsachen, 6.10.2021 (2020/2016(INI)).

196 Die beschränkte nationale Kompetenz der Union in originären kompetenziellen Kernbereichen der Mitgliedstaaten war auch der Grund dafür, dass die DSGVO für den Bereich der behördlichen Datenverarbeitung den Mitgliedstaaten zahlreiche Öffnungsklauseln zugestanden hatte und die Union sich für den Bereich der polizeilichen Datenverarbeitung auf Richtlinien-Vorgaben beschränkte, statt eine Verordnung zu erlassen.

197 Z. B. setzt sich die Kampagne „Reclaim Your Face“ (https://reclaimyourface.eu/de/) auf europäischer Ebene gegen Gesichtserkennung ein. Die deutsche Initiative „Gesichtserkennung stoppen“ (https://gesichtserkennung-stoppen.de/) wirkt mit bei „Reclaim Your Face“ zusammen und findet außer bei dem Chaos Computer Club und der Gesellschaft für Informatik auch bei dem BfDI Ulrich Kleber Unterstützung. In den USA finden sich ebenfalls Organisationen zu diesem Zweck zusammen (https://www.banfacialrecognition.com/).

198 Vgl. u. a. Selinger/Leong, The Ethics of Facial Recognition Technology, in: Véliz (Hrsg.), The Oxford Handbook of Digital Ethics. (Manuskript verfügbar unter: https://dx. doi.org/10.2139/ssrn.3762185), siehe v. a. S. 6 ff.; Smith/Miller, AI & SOCIETY 2021, S. 5 ff. Zu ethischen Fragen der Forschung an Gesichtserkennungstechnologie siehe auch bspw. van Noorden, The ethical questions that haunt facial-recognition research, Nature vom 18.11.2020.