Nadja Braun Binder / Eliane Kunz / Liliane Obrecht

Maschinelle Gesichtserkennung im öffentlichen Raum

Der Einsatz von maschineller Gesichtserkennung im öffentlichen Raum birgt die Gefahr einer gesellschaftlichen Massenüberwachung. Werden dabei biometrische Daten, die ein Individuum eindeutig identifizieren, genutzt, handelt es sich nach dem neuen Datenschutzgesetz um eine Bearbeitung besonders schützenswerter Personendaten. Die maschinelle Gesichtserkennung ist in der Schweiz regulatorisch kaum umrissen. Dabei sind Überlegungen dazu dringend geboten. Dies ergibt sich einerseits aus der Grundrechtsrelevanz der Thematik, andererseits fordern zivil-gesellschaftliche Organisationen ein entsprechendes Verbot. Auch die geplante EU-Regelung zur künstlichen Intelligenz, in der die Gesichtserkennung enthalten ist, sollte in den Erwägungen berücksichtigt werden. Vor diesem Hintergrund gibt der vorliegende Aufsatz einen Überblick über die im Zusammenhang mit maschineller Gesichtserkennung im öffentlichen Raum auftretenden Rechtsfragen und befasst sich mit der Frage der Notwendigkeit eines Verbots oder Moratoriums.

Zitiervorschlag:
NADJA BRAUN BINDER / ELIANE KUNZ / LILIANE OBRECHT, Maschinelle Gesichtserkennung im öffentlichen Raum, sui generis 2022, S. 53

Prof. Dr. iur. Nadja Braun Binder, MBA, Professorin für Öffentliches Recht an der Universität Basel (nadja.braunbinder@unibas.ch). **Eliane Kunz,** Studierende in Assistenzfunktion an der Universität Basel (eliane.kunz@unibas.ch). **Liliane Obrecht,** Wissenschaftliche Mitarbeiterin und Doktorandin an der Universität Basel (liliane.obrecht@unibas.ch). Dieser Aufsatz entstand im Rahmen des von der Mercator Stiftung geförderten Projekts «Nachvollziehbare Algorithmen: Ein Rechtsrahmen für den Einsatz von Künstlicher Intelligenz».

URL: sui-generis.ch/204

DOI: https://doi.org/10.21257/sg.204

I. Einleitung

1 In annähernd 100 Staaten werden Technologien zur Gesichtserkennung verwendet.[1] Gleichzeitig schlägt die EU-Kommission ein grundsätzliches Verbot biometrischer Fernidentifizierungssysteme im öffentlichen Raum vor – wenn auch mit weitreichenden Ausnahmen.[2] In der Schweiz steht das Thema Gesichtserkennung seit Kurzem ebenfalls auf der politischen Agenda.[3] Zudem setzen sich zivilgesellschaftliche Organisationen für ein Verbot maschineller Gesichtserkennung und insbesondere biometrischer Massenüberwachung ein.[4] In der Schweiz ist die juristische Auseinandersetzung mit dem Thema dagegen bislang überschaubar geblieben.[5] Bei den meisten Beiträgen handelt es sich um Zeitungs- oder Blogartikel.[6]

II. Grundlagen

2 Die rechtliche Befassung mit maschineller Gesichtserkennung setzt eine Klärung von deren zentralen Elementen voraus (1.-3.). Zudem soll kurz skizziert werden, wo Gesichtserkennung zum Einsatz kommt (4.).

1. Das Gesicht als Teil biometrischer Daten

3 Biometrische Merkmale sind messbare, körpereigene, physiologische oder verhaltensspezifische Kennzeichen, die einer Person zugeordnet werden können, grundsätzlich einzigartig sind und nur unter grossem Aufwand verändert werden können.[7] Das Gesichtsbild ist ein physiologisches biometrisches Merkmal, das vorgegeben und grundsätzlich unveränderbar ist.[8]

Das revidierte Datenschutzgesetz[9] ordnet die biometrischen Daten, die eine natürliche Person eindeutig identifizieren, der Kategorie der besonders schützenswerten Personendaten zu und verankert den Begriff neu explizit in Art. 5 lit. c Ziff. 4 revDSG. Demnach handelt es sich um Personendaten, «die durch ein spezifisches technisches Verfahren zu den physischen, physiologischen oder verhaltenstypischen Merkmalen eines Individuums gewonnen werden und die eine eindeutige Identifizierung der betreffenden Person ermöglichen oder bestätigen»[10]. Als Beispiele nennt die Botschaft digitale Fingerabdrücke, Gesichtsbilder, Bilder der Iris oder Aufnahmen der Stimme. Zwingend ist, dass diese Daten auf einem Verfahren beruhen, welches die eindeutige Identifizierung oder Authentifizierung einer Person erlaubt.[11] Dies wäre bei unscharfen Bildern oder Teilabdrücken eines Fingers unter Umständen nicht der Fall. 4

2. Maschinelle Gesichtserkennung

Maschinelle Gesichtserkennung kann definiert werden als eine «automatische Verarbeitung digitaler Bilder, die Gesichter von natürlichen Personen enthalten, um bei diesen eine Identifizierung, Authentifizierung bzw. Verifizierung oder Kategorisierung durchzuführen»[12]. 5

Bei der Identifizierung wird das Ermitteln der Identität einer Person aus einer Vielzahl anderer Personen heraus angestrebt – mithin die Beantwortung der Frage, wer eine bestimmte Person ist.[13] Das Authentifizierungs- bzw. Verifizierungsverfahren dient der Identitätsbestätigung einer Person, also der Abklärung, ob eine Person tatsächlich diejenige ist, als die sie sich ausgibt. 6

1 Siehe dazu die Übersichtskarte des britischen Unternehmens Surfshark, The Facial Recognition World Map.

2 Europäische Kommission, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union vom 21. April 2021, COM(2021) 206 (EU-KI-Verordnungsentwurf).

3 Bund: Vorstoss NR Glättli vom 5. Mai 2021 (21.3580). Basel-Stadt: Anzug Baumgartner und Konsorten vom 13. Januar 2022 (22.5022). Stadt Zürich: Postulat Maggi/Wey vom 17. November 2021 (2021/451) und Motion vom 17. November 2021 (2021/450). Stadt Lausanne: Postulat Gaillard vom 23. November 2021 (Dépôt N°8/07.12.2021) und projets de règlement No8/07.12.2021.

4 Petition «Gesichtserkennung stoppen» von AlgorithmWatch, Amnesty International und Digitale Gesellschaft Schweiz.

5 Siehe etwa MONIKA SIMMLER / GIULIA CANOVA, Gesichtserkennungstechnologie: Die «smarte» Polizeiarbeit auf dem rechtlichen Prüfstand, Sicherheit & Recht 2021, S. 105 ff.; RAMONA KEIST, Gesichtserkennung im zivilrechtlichen Persönlichkeitsschutz, Jusletter vom 30. Mai 2019; LIVIA MATTER, Gesichtserkennung auf dem Vormarsch, digma 2019, S. 14 ff.

6 Siehe z. B. SIMONE LUCHETTA, So jagen Schweizer Polizisten mit Gesichtserkennung Verbrecher, Tagesanzeiger vom 17. April 2021; MARTIN STEIGER, Gesichtserkennung: Drei populäre datenschutzrechtliche Irrtümer, 21. November 2021; MICHAL CICHOCKI, Europarat veröffentlicht Leitlinien zu Gesichtserkennung (Guidelines on facial recognition), LawBlogSwitzerland vom 4. April 2021.

7 EDÖB, Leitfaden zu biometrischen Erkennungssystemen, 2009, S. 5; DOMINIKA BLONSKI, Biometrische Daten als Gegenstand des informationellen Selbstbestimmungsrechts, Bern 2015, S. 6; privatim, Leitfaden zur datenschutzrechtlichen Beurteilung von biometrischen Verfahren, 2005, S. 3.

8 BLONSKI (Fn. 7), S. 8. Auf Veränderungen des Gesichtsbildes mittels chirurgischer Eingriffe, durch Krankheiten, Unfälle oder Wachstum wird hier nicht näher eingegangen.

9 Das Bundesgesetz über den Datenschutz vom 19. Juni 1992 (DSG; SR 235.1) wurde revidiert. Das revidierte Datenschutzgesetz vom 25. September 2020 (revDSG) tritt voraussichtlich am 1. September 2023 in Kraft. Die weiteren Ausführungen werden auf die Rechtslage nach dem revDSG gestützt, wobei auch Bezug auf bisherige Literatur genommen wird, soweit die entsprechenden Ausführungen auch auf die Rechtslage nach dem revDSG zutreffen.

10 Botschaft vom 15. September 2017 zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz (BBl 2017 6941), S. 7020.

11 Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz (Fn. 10), S. 7020.

12 Artikel-29-Datenschutzgruppe, Stellungnahme 02/2012 zur Gesichtserkennung bei Online- und Mobilfunkdiensten vom 22. März 2012, 00727/12/DE, WP 192, Brüssel, S. 2.

13 EDÖB (Fn. 7), S. 5; zur Technik der Gesichtserkennung vertieft GÜNTER KARJOTH, Fähigkeiten der Gesichtserkennung, digma 2019, S. 6 ff.

7 Die im Zusammenhang mit maschineller Gesichtserkennung auftretenden Rechtsfragen stellen sich grundsätzlich unabhängig davon, welche konkrete Technologie eingesetzt wird und ob man in diesem Zusammenhang von künstlicher Intelligenz (KI) spricht.[14] Zentral sind vielmehr die damit einhergehende Gefahr der Massenüberwachung, die eine breit angelegte, staatliche Überwachung der Bevölkerung meint, sowie der Umstand, dass biometrische Daten bearbeitet werden.

3. Definition des öffentlichen Raumes

8 In der Schweiz existiert keine gesetzliche Definition des öffentlichen Raumes. In der Literatur wird vorgeschlagen, den Begriff «Raum» als nicht abgeschlossene bzw. nicht fest eingegrenzte Ausdehnung zu verstehen.[15] Öffentlichkeit kann als der Allgemeinheit zugänglich und benutzbar interpretiert werden, unabhängig davon, ob das Eigentum am Raum in öffentlicher oder privater Hand liegt.[16] Die EU-Kommission definiert in Art. 3 Nr. 39 EU-KI-Verordnungsentwurf den öffentlich zugänglichen Raum als «einen der Öffentlichkeit zugänglichen physischen Ort, unabhängig davon, ob dafür bestimmte Zugangsbedingungen gelten».

9 Für die Zwecke des vorliegenden Aufsatzes wird der öffentliche Raum in Anlehnung an die oben skizzierten Definitionen als ein für Personen physisch zugänglicher Ort verstanden, unabhängig davon, ob dafür bestimmte Zugangsbedingungen gelten und unabhängig der Eigentumsverhältnisse. Der Cyberspace bzw. das Internet werden nicht zum physisch zugänglichen Raum gezählt und damit Erwägungen zur Online-Überwachung ausgeklammert.

4. Einsatzbereiche

a) Echtzeit-Gesichtserkennung

10 Gesichtserkennungssysteme können in Echtzeit Daten aus Überwachungskameras zur Identifizierung oder Verifizierung bestimmter Personen auswerten. Diese Möglichkeit wird etwa im Rahmen von automatisierten Passkontrollen an Flughäfen genutzt, indem biometrische Erkennungsmerkmale des Gesichts mit den auf dem Pass gespeicherten Daten abgeglichen werden. Die Daten können ausserdem registriert sowie mithilfe von Fahndungs- und Informationssystemen überprüft werden.[17]

11 Ein weiterer denkbarer Einsatzbereich in der Schweiz könnte in Zukunft die Zutrittskontrolle zu Sportstadien sein. Mithilfe maschineller Gesichtserkennung sollen registrierte Hooligans direkt beim Eingang erkannt werden.[18] Solche Systeme wurden und werden international bereits eingesetzt.[19] In der Schweiz hat ein Start-up ausserdem im Sommer 2021 die Idee lanciert, das Vorhandensein des Covid-Zertifikats mittels Gesichtserkennung zu prüfen.[20]

12 Echtzeit-Gesichtserkennung kommt in Europa vereinzelt zum Einsatz, um bestimmte, geografisch eingegrenzte Gebiete zu überwachen. Die gescannten Gesichter werden mit Überwachungslisten der Polizei oder der Gerichte abgeglichen.[21]

13 Vermehrt setzen auch Private in Europa Gesichtserkennung ein, wie z. B. Einkaufsgeschäfte,[22] die mithilfe von Gesichtserkennung Personen, die in der Vergangenheit gestohlen oder sich nicht regelkonform verhalten haben, beim Betreten des Geschäfts erfassen und dem Personal melden.[23] Ein ähnliches Phänomen ist in den USA zu beobachten, wo lokale Geschäfte Überwachungskameras installieren, die ihre Aufnahmen in Echtzeit an die Polizei übermitteln, die diese daraufhin durch Fahndungs- und

14 GERRIT HORNUNG / STEPHAN SCHINDLER, Datenschutz bei der biometrischen Gesichtserkennung, Datenschutz und Datensicherheit, 2021, S. 515 ff.

15 Siehe PATRICE MARTIN ZUMSTEG, Demonstrationen in der Stadt Zürich, Zürich 2020, S. 6 f.

16 ZUMSTEG (Fn. 15), S. 7.

17 Dies ist der Fall am Basler und Genfer Flughafen. Es ist anzumerken, dass die französische Grenzpolizei die Betreiberin dieser Geräte ist, was auf einen Staatsvertrag zwischen der Schweiz und Frankreich zurückzuführen ist. Dazu DANIEL BALLMER, Ein Scan fürs Gesicht: Der Basler Euro-Airport beschleunigt die Passkontrolle, bz vom 9. Februar 2019; Genève aéroport communiqués, Genève aéroport teste le contrôle automatisé à la frontière vom 5. Dezember 2019. Am Flughafen Zürich hingegen findet keine solche Registrierung und Abgleichung statt, nur während eines Pilotprojekts im Jahr 2003; vgl. dazu den Regierungsratsbeschluss Nr. 447/2021, Auszug aus dem Protokoll des Regierungsrates des Kantons Zürich, Sitzung vom 5. Mai 2021, KR-Nr. 128/2021, S. 2. Zu einer Übersicht über Europa vgl. CHARLES LIEBHERR, Gesichtserkennung: Einführung durch die Hintertür, Eine Studie im Auftrag der Grünen Fraktion im EU-Parlament zum Einsatz von Gesichtserkennung in Europa, Schweizer Radio und Fernsehen (SRF), Echo der Zeit vom 25. Oktober 2021.

18 Siehe zu Bern: Vadiant.net AG bzw. fussball.ch, Pilotprojekt mit Gesichtserkennung; zum Kanton Wallis: JULIEN CALOZ, Gesichtserkennung beim FC Sion? Datenschützer hätte nichts dagegen, Watson vom 15. Juli 2021.

19 Siehe z. B. zu Dänemark: SIDSEL OVERGAARD, A Soccer Team In Denmark Is Using Facial Recognition To Stop Unruly Fans, NPR vom 21. Oktober 2019.

20 HANS JÖRG MARON, Schweizer Startup kombiniert Covid-Zertifikat-Scan mit Gesichtserkennung, inside channels vom 3. November 2021. Bis zur Aufhebung der COVID-Massnahmen im Februar 2022 wurde der Covid-Checker im Hotel Dolder in Zürich eingesetzt, vgl. dazu MARTIN HUBER, Dolder Grand setzt auf Gesichtserkennung, Zürcher Tagblatt vom 24. November 2021.

21 Siehe etwa zu Grossbritannien: HANNA ZIADY, London will use live facial recognition cameras to police the city, CNN vom 24. Januar 2020.

22 Zu den Einsatzmöglichkeiten und Grenzen von Gesichtserkennung im Detailhandel vgl. MATTHIAS GLATTHAAR, Gesichtserkennung im Supermarkt?, digma 2019, S. 20 ff.

23 Siehe z. B. zu Grossbritannien: GARETH LEWIS, Protecting our customers and colleagues, facewatch vom 5. Oktober 2020.

Führerschein-Datenbanken laufen lässt und so virtuelle Patrouillen durchführt.[24] Ob bzw. in welchem Umfang Gesichtserkennung in der Schweiz im Einzelhandel und in Einkaufszentren eingesetzt wird, ist unklar.[25]

b) Nachträgliche Gesichtserkennung

14 Bei der nachträglichen Gesichtserkennung geht es um den Einsatz einer Gesichtserkennungssoftware im Nachgang zu einer Foto- oder Videoaufnahme – oftmals nach einer Straftat und während der Strafverfolgung.[26] In der Schweiz setzt die Polizei vereinzelt Gesichtserkennung zum Abgleich von Fahndungsbildern ein, wobei eine kantonale Polizeidatenbank bekannter Straftäterinnen und Straftäter mit einer anderen, bspw. kantonsübergreifenden Datenbank, abgeglichen wird.[27] Die Fahndungsbilder stammen oft aus Überwachungskameras von Geschädigten, wie z. B. eines bestohlenen Kleiderladens. Die konkrete Identifizierung der verdächtigten Person obliegt nach wie vor einer Polizistin oder einem Polizisten und nicht einer Software.[28]

15 Nachträgliche Gesichtserkennung wird auch im internationalen Kontext insbesondere im Polizeibereich eingesetzt. Interpol nutzt seit 2016 Gesichtserkennung mit einer Gesichtsbilderdatenbank von Personen aus über 179 Staaten zur Identifizierung und Verifizierung; die Ergebnisse werden anschliessend von Hand überprüft.[29] In Europa wie auch den USA wird in vereinzelten Staaten bzw. Städten nachträgliche Gesichtserkennung ausserdem eingesetzt, um bei Verdacht auf eine vorsätzlich begangene Straftat einen nachträglichen digitalen Abgleich von Bildern von Überwachungskameras oder Handy-Aufnahmen mit einer Polizeidatenbank durchzuführen.[30] Einsatzszenarien sind bspw. eskalierte Demonstrationen.[31]

c) Exkurs: Verzicht auf maschinelle Gesichtserkennung

16 Die erwähnten Beispiele bedeuten nicht, dass weltweit eine lineare Zunahme des Einsatzes von maschineller Gesichtserkennung zu verzeichnen wäre. Vielmehr gibt es verschiedene Länder und Städte, in denen Gesichtserkennung inzwischen verboten oder Pilotversuche sistiert wurden. So etwa in Deutschland, wo Rechtsgrundlagen für die Durchführung von Gesichtserkennung an über hundert deutschen Bahnhöfen und Flughäfen im Entwurfsstadium verworfen wurden.[32] Auch am Brüsseler Flughafen Zaventem wurde über mehrere Jahre im Rahmen eines Pilotprojekts eine Gesichtserkennungstechnologie eingesetzt, was aufgrund eines nun geltenden landesweiten Verbotes allerdings wieder eingestellt wurde.[33] In Grossbritannien wurde Gesichtserkennung an Schulen eingesetzt, um angesichts der Corona-Pandemie eine kontaktlose Bezahlung des Mittagessens zu ermöglichen. Nach breiter Kritik stellten die Schulen dieses System (vorerst) wieder ein.[34] Auch in den USA haben einige Städte den Einsatz von Gesichtserkennung, zumindest durch staatliche Behörden, verboten.[35]

24 Projekt «Green Light» in Detroit, vgl. CHRISTOPHER JONES, Law enforcement use of facial recognition: bias, disparate impacts on people of color, and the need for federal legislation, North Carolina Journal of Law & Technology 2021, S. 790.

25 Studie von AlgorithmWatch Schweiz, Kennt der Supermarkt Ihr Gesicht?, 18. November 2021; zudem weiter BERNHARD ODEHNAL, Spionagefirma bietet Gesichtserkennung von Shoppern an, Tagesanzeiger vom 19. November 2021.

26 SIMMLER/CANOVA (Fn. 5), S. 8 ff.

27 Vgl. für weitere Informationen zu den einzelnen Gesichtserkennungssoftwares LUCHETTA (Fn. 6). Für Aufruhr sorgte auch die Verwendung der Gesichtserkennungssoftware «Clearview AI» durch einige Angehörige der Stadtpolizei Zürich, die interne Testuntersuchungen durchführten, sie allerdings nicht für Strafverfolgungszwecke einsetzten; vgl. dazu SIMONE LUCHETTA, Zürcher Stadtpolizist testete Clearview nach einer Ausbildung, Tagesanzeiger vom 6. September 2021.

28 DANIEL GERNY, Wie intelligente Kameras in der Schweiz Einzug halten, NZZ online vom 22. Juni 2018; THOMAS SCHWENDENER, Facial Recognition soll bald St. Galler Polizei unterstützen, Inside IT vom 18. Juni 2020.

29 Interpol, Facial Recognition. Darüber hinaus wurde Clearview auch von der Interpol-Einheit «Verbrechen gegen Kinder» mit einem 30-tägigen Testkonto getestet, um die Opfer von sexuellem Kindesmissbrauch im Internet zu identifizieren; vgl. dazu PHILIPP ANZ, Wer alles die Gesichtserkennung von Clearview testete, Inside IT vom 30. August 2021.

30 Siehe zu Österreich: Beantwortung der parlamentarischen Anfrage «Gesichtsbilderdatenbanken der österreichischen Sicherheitsbehörden» 750/AB 1 zu 708/J (XXVII. GP); Salzburger Nachrichten vom 4. Mai 2021 (Amnesty will Ende der Gesichtserkennung in Österreich); zu Grossbritannien: Metropolitan Police, Facial Recognition; zu den USA: NYPD, Questions and Answers Facial Recognition.

31 MARKUS SULZBACHER, Polizei nutzt neue Gesichtserkennung, um Demonstranten zu identifizieren, Der Standard vom 15. September 2020.

32 Der Spiegel vom 24. Januar 2020 (Seehofer verzichtet auf Software zur Gesichtserkennung). Mittlerweile wurde der gesamte Gesetzesentwurf abgelehnt.

33 Im Rahmen der Anpassung des Gesetzes über die Installation und Nutzung von Überwachungskameras (Loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance) wurde im März 2018 ein Art. 8/1 eingeführt, der jegliche Überwachungskameras gekoppelt mit Registern oder Dateien mit personenbezogenen Daten verbietet, sofern sie nicht ausschliesslich zur automatischen Erkennung von Kfz-Kennzeichen eingesetzt werden und der Datenschutz gewährleistet ist. Siehe dazu Art. 78 Belgisch Staatsblad vom 16. April 2018, S. 33708.

34 HANS JÖRG MARON, Britische Schulen: Schon wieder Schluss mit Gesichtserkennung, Inside IT vom 26. Oktober 2021.

35 Darunter San Francisco, das im Kontext der Einführung einer Verordnung zur Anschaffung von Überwachungstechnik (Ordinance 190110, Administrative Code – Acquisition of Surveillance Technology) den Einsatz von Gesichtserkennungstechnologien (mit begrenzten Ausnahmen) verbietet und eine öffentliche Bekanntgabe aller verwendeten Überwachungstechnologien vorsieht. Die Verordnung definiert Gesichtserkennungstechnologie als ein automatisiertes oder halbautomatisiertes Verfahren, das dabei hilft, die Identifizierung oder Verifizierung einer Person anhand ihres Gesichts vorzunehmen – somit dürfte die Echtzeit-Gesichtserkennung wie auch die nachträgliche Gesichtserkennung darunter gefasst sein. Verboten auch in Oakland, Berkeley, Portland, Boston und Somerville, vgl. RACHEL METZ, Portland passes broadest facial recognition ban in the US, CNN vom 10. September 2020.

III. Rechtliche Würdigung

1. Datenschutzrechtliche Vorgaben

17 Das Datenschutzrecht statuiert einige Definitionen, Grundsätze und Pflichten, die für eine Datenbearbeitung sowohl durch Private als auch Behörden gelten.[36] Ausgangspunkt einer Datenbearbeitung bildet deren Rechtmässigkeit (Art. 6 Abs. 1 revDSG). Weiter muss eine Datenbearbeitung verhältnismässig sein (Art. 6 Abs. 2 revDSG). Das bedeutet, dass Daten nur bearbeitet werden dürfen, sofern ihre Bearbeitung geeignet ist, den verfolgten Zweck zu erfüllen und wenn kein milderes Mittel zur Zweckerreichung zur Verfügung steht.[37] Schliesslich muss die Datenbearbeitung zumutbar sein, dementsprechend muss ein vernünftiges Verhältnis zwischen der Datenbearbeitung und dem Eingriff in die Privatsphäre der betroffenen überwachten Personen bzw. dem Grundrechtseingriff bestehen.[38] Gerade im Bereich des Einsatzes von Gesichtserkennung im öffentlichen Raum zum Schutz der öffentlichen Ordnung und Sicherheit vor Störungen – z. B. die Verhinderung von Vandalismus oder Littering – dürfte sich regelmässig ein milderes Mittel finden lassen, wie etwa baulich-technische oder polizeilich-organisatorische Massnahmen.[39] Aus dem Grundsatz der Verhältnismässigkeit werden zudem die Prinzipien der Datenvermeidung und der Datensparsamkeit abgeleitet.[40] Da im Grundsatz davon ausgegangen werden kann, dass maschinelle Gesichtserkennungssysteme sehr viele (Trainings-)Daten benötigen, um treffsichere Outputs generieren zu können,[41] steht die Technologie in einem Spannungsverhältnis zu den soeben genannten Prinzipien. Zudem stellt sich dabei grundsätzlich die Frage, ob und inwieweit Trainingsdaten überhaupt datenschutzkonform erhoben und genutzt werden können.

18 Mit der Verhältnismässigkeit hängen ferner die Grundsätze der Zweckbindung und der Erkennbarkeit zusammen (Art. 6 Abs. 3 revDSG). Bei einer Datenbearbeitung muss stets der Bearbeitungszweck festgelegt und eingehalten werden. Insbesondere der Einsatz maschineller Gesichtserkennung zur allgemeinen Gefahrenabwehr kann dazu führen, dass die Festlegung des Bearbeitungszwecks untergraben wird, da dadurch vielseitige und breite Analysemöglichkeiten geschaffen werden, die vom Bearbeitungszweck abweichen.[42] Der Zweck der Bearbeitung weist auch eine zeitliche Komponente auf. Mithin müssen Daten vernichtet werden, sobald sie zum Bearbeitungszweck nicht mehr erforderlich sind (Art. 6 Abs. 4 revDSG). Somit ist die Speicherungsdauer festzulegen.[43]

19 Die skizzierten Anforderungen gelten bereits für das Erheben der Daten im öffentlichen Raum (z. B. CCTV-Kameraaufnahmen von Passantinnen und Passanten) und nicht erst für die Überprüfung ebendieser mittels Gesichtserkennung. Die Datenbeschaffung sowie insbesondere der Bearbeitungszweck müssen ausserdem für die betroffene Person erkennbar sein. Das revDSG führt mit Art. 19 ausgeweitete Informationspflichten bei der Beschaffung von Personendaten ein, die für Private und Behörden gelten. Unter bestimmten Voraussetzungen, etwa wenn die Person bereits über die entsprechenden Informationen verfügt oder die Bearbeitung gesetzlich vorgesehen ist, entfällt die Informationspflicht (Art. 20 Abs. 1 lit. a und b revDSG). Diese Bestimmung ist allerdings explizit als Ausnahme konstituiert.[44] Die Erkennbarkeit wird subsidiär, sofern Informationspflichten bestehen.[45] Die Information muss angemessen sein und diejenigen Informationen enthalten, die die betroffene Person benötigt, um ihre Rechte gemäss Datenschutzrecht geltend machen zu können (Art. 19 Abs. 2 lit. a-c revDSG). Die Botschaft zum revDSG hält fest, dass bei der Wahl einer allgemeinen Informationsform der Zugang zur Information einfach, die Information vollständig und der Hinweis augenfällig sein muss.[46] Ein allgemeines Hinweisschild, dass Gesichtserkennung eingesetzt wird, dürfte vor diesem Hintergrund somit als unvollständig und ungenügend zu bewerten sein.

20 Zu erwähnen ist ferner der Grundsatz der Datenrichtigkeit (Art. 6 Abs. 5 revDSG), der die Vollständigkeit und die Aktualität der Daten umfasst.[47] Die Pflicht zur Richtigkeit ist allerdings nicht absolut zu verstehen, sie muss

36 Zu den datenschutzrechtlichen Grundsätzen im Kontext der Videoüberwachung ausführlich LUCIEN MÜLLER, Videoüberwachung in öffentlich zugänglichen Räumen – insbesondere zur Verhütung und Ahndung von Straftaten, Zürich 2011, S. 60 ff.

37 BGE 138 II 346 E. 9.2; das Verhältnismässigkeitsprinzip im Datenschutzrecht gilt nicht nur für staatliches Handeln gemäss Art. 5 Abs. 2 BV (Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 [BV; SR 101]), sondern auch unter Privaten, was zu hohen Anforderungen an eine Datenbearbeitung führt, vgl. BAERISWYL, in: Baeriswyl/Pärli (Hrsg.), Stämpfli Kommentar, Datenschutzgesetz, Bern 2015, Art. 4 N 25 (zit. SHK DSG-BEARBEITERIN)

38 Zum datenschutzrechtlichen Verhältnismässigkeitsprinzip ASTRID EPINEY, § 9 Allgemeine Grundsätze, in: Belser/Epiney/Waldmann (Hrsg.), Datenschutzrecht, Bern 2011, S. 528 ff.

39 Vgl. z. B. den Bericht der Kantons- und Stadtentwicklung Basel-Stadt zur Schaffung von Sicherheit öffentlicher Räume vom September 2018, S. 56.

40 SHK DSG-BAERISWYL, Art. 4 N 23.

41 KARJOTH (Fn. 13), S. 11.

42 SIMMLER/CANOVA (Fn. 5), S. 109, betiteln dies als eine «anlasslose und verdachtsunabhängige Massnahme mit grosser Streubreite».

43 MÜLLER (Fn. 36), S. 230 f.

44 Für Behörden wird die Ausnahme zur Regel, da eine Datenbearbeitung gestützt auf das Legalitätsprinzip stets eine gesetzliche Grundlage voraussetzt. Diese Lösung ist allerdings insbesondere mit Blick auf die Adressatengerechtigkeit der Information kritisch zu sehen, vgl. FLORENT THOUVENIN / NADJA BRAUN BINDER, Transparenz durch Datenschutzerklärungen von Behörden, ZSR 141/2022 I, S. 5 ff.

45 SHK DSG-BAERISWYL, Art. 4 N 47.

46 Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz (Fn. 10), S. 7050 f.

47 SHK DSG-BAERISWYL/BLONSKI, Art. 5 N 1.

vielmehr in einem angemessenen Verhältnis zum Verarbeitungszweck stehen (relative Datenrichtigkeit).[48] Gefordert wird, dass mit Rücksicht auf den Zweck alle geeigneten Massnahmen ergriffen werden, die eine Berichtigung, Löschung oder Vernichtung unrichtiger oder unvollständiger Daten ermöglichen.[49] Im Kontext der Gesichtserkennung ist eine sehr hohe Wahrscheinlichkeit der richtigen Identifizierung bzw. Verifizierung der Betroffenen für die Zulässigkeit eines biometrischen Verfahrens zu fordern.[50] Um dies zu erreichen, müssen die Trainingsdatensätze insbesondere eine hinreichende Diversität bezüglich Alter, Geschlecht und Hautfarbe aufweisen.[51]

2. Gesichtserkennung im öffentlichen Raum durch Private

21 Die Bearbeitung von Personendaten durch Private fällt grundsätzlich unter das Datenschutzgesetz (Art. 2 Abs. 1 lit. a revDSG), sofern die Bearbeitung nicht ausschliesslich dem persönlichen Gebrauch dient (Art. 2 Abs. 2 lit. a revDSG). Ein rein persönlicher Gebrauch ist beim Einsatz von maschineller Gesichtserkennung im öffentlichen Raum regelmässig auszuschliessen, da das gesammelte Bildmaterial in der Regel Überwachungszwecken und damit potenziell auch als Beweismittel im Rahmen eines späteren Straf- oder Zivilverfahrens dient.[52]

22 Die Datenbearbeitung durch private Personen darf keine widerrechtliche Persönlichkeitsverletzung darstellen (Art. 6 Abs. 1 i. V. m. Art. 30 Abs. 1 revDSG). Folglich ist eine Datenbearbeitung nur zulässig, sofern die Grundsätze des Datenschutzrechts (Art. 30 Abs. 2 lit. a revDSG) eingehalten werden,[53] maschinelle Gesichtserkennung nicht gegen den ausdrücklichen Willen der Betroffenen eingesetzt wird (Art. 30 Abs. 2 lit. b revDSG) oder ein Rechtfertigungsgrund (Art. 31 Abs. 1 revDSG) vorliegt. Für die Bearbeitung biometrischer Daten i. S. v. Art. 5 lit. c Ziff. 4 revDSG ist grundsätzlich eine ausdrückliche Einwilligung der betroffenen Person notwendig (Art. 6 Abs. 7 lit. a revDSG). Die Einwilligung muss freiwillig erfolgen und es muss eine vorgängige Information über die Datenbearbeitung stattfinden (Art. 6 Abs. 6 und 7 i. V. m. Art. 19 Abs. 1 revDSG). Obwohl die Ausdrücklichkeit der Einwilligung keine Schriftlichkeit voraussetzt, muss der Wille der betroffenen Person eindeutig aus den Umständen des Einzelfalles hervorgehen.[54] Sowohl die Informationspflicht als auch die ausdrückliche und freiwillige Einwilligung sind bei der maschinellen Gesichtserkennung im öffentlichen Raum schwer umzusetzen.[55] Würde bspw. das Betreten öffentlicher Räume jeweils von einer Einwilligung in die Gesichtserkennung abhängig gemacht, wäre die Freiwilligkeit nicht gegeben.[56]

23 Als Rechtfertigungsgründe für eine widerrechtliche Persönlichkeitsverletzung – z. B. die Bearbeitung biometrischer Daten ohne ausdrückliche Zustimmung der betroffenen Person – kommen ein überwiegendes privates oder öffentliches Interesse oder das Vorliegen einer gesetzlichen Grundlage in Frage (Art. 31 Abs. 1 revDSG). Analog zur Einschätzung des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) hinsichtlich der Videoüberwachung dürfte allerdings auch mit Blick auf den Einsatz maschineller Gesichtserkennung davon auszugehen sein, dass die Überwachung des öffentlichen Raums durch Private zur Wahrung privater Interessen regelmässig eine Persönlichkeitsverletzung darstellt, da kein überwiegendes Interesse vorhanden ist.[57] Es können zwar keine verallgemeinernden Aussagen bezüglich der Interessenabwägung gemacht werden, da diese immer konkret und einzelfallspezifisch erfolgt.[58] Jedoch sind Konstellationen, in denen das private Interesse an der Überwachung des öffentlichen Raumes das Interesse der betroffenen Personen am Schutz ihrer biometrischen Daten i. S. v. Art. 5 lit. c Ziff. 4 revDSG und damit am Schutz besonders schützenswerter Daten überwiegt, praktisch nicht vorstellbar. Ferner kann auch die Wahrung von Sicherheit und Ordnung (als öffentliches Interesse) im öffentlichen Raum nicht als Rechtfertigungsgrund für den Einsatz von maschineller Gesichtserkennung durch Private herangezogen werden. Denn die Wahrung von Sicherheit und Ordnung im öffentlichen Raum ist Sache der Polizei und weiterer Behörden.

24 Bezüglich der allgemeinen Videoüberwachung werden zwei Ausnahmen statuiert:[59] Erstens bei Vorliegen einer an sich rechtmässigen Überwachung von privatem Grund,

48 MAURER-LAMBROU/SCHÖNBÄCHLER, in: Maurer-Lambrou/Blechta (Hrsg.), Basler Kommentar, Datenschutzgesetz, Öffentlichkeitsgesetz, 3. Aufl., Basel 2014, Art. 5 N 6 (zit. BSK DSG-BEARBEITERIN).

49 SYLVAIN MÉTILLE, Le traitement de données personnelles sous l'angle de la nouvelle loi fédérale sur la protection des données du 25 septembre 2020, SJ II/2021, S. 11.

50 Privatim (Fn. 7), S. 12.

51 KARJOTH (Fn. 13), S. 11. Dies ist insb. auch wichtig im Hinblick auf das Diskriminierungsverbot, dazu Rz. 25 ff.

52 LUCIEN MÜLLER, Private Videoüberwachung in öffentlich zugänglichen Räumen – Datenschutzrechtliche Aspekte, Sicherheit & Recht 2012, S. 65.

53 Vgl. dazu Rz. 17 ff., wobei insb. der Grundsatz der Verhältnismässigkeit zu betonen ist.

54 SHK DSG-BAERISWYL, Art. 4 N 69 ff.

55 Zur Informationspflicht im Rahmen der Gesichtserkennung siehe Rz. 17 ff.

56 MÜLLER (Fn. 52), S. 73 f.; SHK DSG-BAERISWYL, Art. 13 N 65 ff.

57 EDÖB, Videoüberwachung des öffentlichen Raums durch Privatpersonen.

58 SHK DSG-WERMELINGER, Art. 13 N 12.

59 Zum Ganzen EDÖB (Fn. 57). Siehe auch LIZ FISCHLI-GIESSER, Private Videoüberwachung im kommunalen öffentlichen Raum, KPG Bulletin 03/2016, S. 82 ff.

bei der eine geringfügige Miterfassung des öffentlichen Raumes erfolgt und die Überwachung des privaten Grundes nicht anders durchführbar ist. Zweitens bei einer privaten Überwachung des öffentlichen Raumes aus Sicherheitsgründen, die mit dem zuständigen Gemeinwesen vereinbart wurde. Soweit es sich bei der maschinellen Gesichtserkennung um eine Bearbeitung von besonders schützenswerten Personendaten handelt, ist fraglich, ob die mit Blick auf die allgemeine Videoüberwachung statuierten Ausnahmen analog anwendbar wären. Davon ist jedenfalls nicht ohne Weiteres auszugehen.

3. Gesichtserkennung im öffentlichen Raum durch staatliche Behörden

25 Setzen Behörden[60] Gesichtserkennungssoftware ein, müssen sie die Grundrechte berücksichtigen (Art. 35 Abs. 1 BV). Im Kontext maschineller Gesichtserkennung sind dabei insbesondere das Recht auf informationelle Selbstbestimmung (Art. 13 Abs. 2 BV), das Diskriminierungsverbot (Art. 8 Abs. 2 BV) und die Meinungs- und Versammlungsfreiheit (Art. 16 und 22 BV) zu berücksichtigen.

a) Informationelle Selbstbestimmung

26 Art. 13 Abs. 1 BV schützt unter anderem in der Öffentlichkeit vorgenommene Handlungen oder Äusserungen, die der Pflege persönlicher Kontakte dienen und mithin Ausdruck der Persönlichkeit sind, ganz allgemein vor Videoüberwachung im öffentlichen und privaten Raum sowie dauernder Beobachtung und Dokumentation in der Öffentlichkeit.[61] Der Schutzbereich des sog. Rechts auf informationelle Selbstbestimmung gemäss Art. 13 Abs. 2 BV umfasst u. a. den Schutz vor bzw. die Entscheidungsfreiheit bzgl. jeglichen staatlichen Umgangs mit den eigenen Personendaten, ein Recht am eigenen Bild, sowie die Autonomie betreffend die eigene gesellschaftliche und soziale Rolle.[62]

27 Das Recht auf informationelle Selbstbestimmung wird durch das Datenschutzrecht konkretisiert. Ausgangspunkt bildet wiederum die Rechtmässigkeit der Datenbearbeitung nach Art. 6 Abs. 1 revDSG. Für Bundesbehörden setzt die Rechtmässigkeit eine formell gesetzliche Grundlage nach Art. 34 Abs. 2 lit. a revDSG voraus, da es um besonders schützenswerte Personendaten geht. Dadurch werden zugleich die verfassungsrechtlichen Anforderungen gem. Art. 36 Abs. 1 BV bestätigt.[63]

28 Neben einer genügenden Normstufe ist auch eine ausreichende Normdichte, mithin eine hinreichend bestimmte gesetzliche Regelung, notwendig.[64] Erforderlich sind die Definition des konkreten Bearbeitungszwecks, die beteiligten Organe, die Kategorien der bearbeiteten Daten und die grobe Umschreibung des Bearbeitungsumfangs.[65] Der pauschale Verweis auf die Gewährleistung der öffentlichen Sicherheit, den Schutz von Personen oder die polizeiliche Aufgabenerfüllung ist nicht ausreichend.[66] Nicht zu vergessen ist zudem die Notwendigkeit einer ausreichenden Rechtsgrundlage für jene Daten, die in den Überwachungsdatenbanken enthalten sind, also die Bilder derjenigen Personen, nach denen bspw. gefahndet wird.[67]

29 Bis dato ist keine gesetzliche Grundlage für die Gesichtserkennung in der Strafprozessordnung[68] oder im kantonalen Polizeirecht auszumachen.[69] Eine gesetzliche Grundlage in einem anderen Rechtsbereich ist z. B. die frühere Verordnung über den Einsatz eines biometrischen Gesichtserkennungssystems am Flughafen Zürich

60 Das Datenschutzrecht des Bundes entfaltet keine Wirkung für kantonale oder kommunale Behörden (Art. 2 Abs. 1 revDSG *e contrario*). Deshalb wird hier (auch) auf verfassungsrechtliche Vorgaben Bezug genommen.

61 BREITENMOSER, in: Ehrenzeller/Schindler/Schweizer/Vallender (Hrsg.), St. Galler Kommentar, Die schweizerische Bundesverfassung, Zürich 2014, Art. 13 N 15 ff. Ausführungen zu internationalen Normen, insb. Art. 8 EMRK (Europäische Menschenrechtskonvention vom 4. November 1950 [EMRK; SR 0.101]), werden in diesem Aufsatz ausgeklammert.

62 MÜLLER (Fn. 36), S. 122 f.

63 Auch gem. Art. 164 Abs. 1 BV ergibt sich die Notwendigkeit einer formell gesetzlichen Grundlage, da die Bearbeitung besonders schützenswerter Personendaten Gefahren für die Persönlichkeit birgt, siehe BSK DSG-UDVARY/BALLENEGGER, Art. 17 N 25. Zudem ist die Notwendigkeit der demokratischen Legitimation von maschineller Gesichtserkennung im öffentlichen Raum zu betonen, siehe MÜLLER (Fn. 36), S. 203 ff., siehe auch BGE 146 I 11 E. 2.3, in dem das Bundesgericht die automatische Fahrzeugfahndung und Verkehrsüberwachung vor dem Hintergrund der seriellen und simultanen Verarbeitung grosser und komplexer Datensätze innert Sekundenschnelle sowie der Möglichkeit der Erstellung von Persönlichkeits- und Bewegungsprofilen als schweren Grundrechtseingriff qualifiziert hat. Analoges gilt für die Gesichtserkennung im öffentlichen Raum. Ein schwerer Grundrechtseingriff durch Gesichtserkennung wird auch in DAVID GJON, Gesichtserkennung: «Ende der Privatsphäre», plädoyer 6/2021, S. 27, angenommen.

64 Dazu ausführlich MÜLLER (Fn. 36), S. 203 ff. Vgl. auch ESTHER ZYSSET, Brauche ich für meine KI-Anwendung eine gesetzliche Grundlage und wenn ja, welcher Art?, Public Sector Law vom 22. September 2021.

65 BSK DSG-UDVARY/BALLENEGGER, Art. 17 N 19.

66 FLORIAN SAMUEL FLEISCHMANN, Polizeirechtliche Massnahmen zur Bekämpfung der Gewalt anlässlich von Sportveranstaltungen, Zürich 2019, S. 282 f.

67 Zu dieser Unterscheidung und den daraus resultierenden Anforderungen an die gesetzliche Grundlage siehe SIMMLER/CANOVA (Fn. 5), S. 15 ff.; ferner FRA – European Union Agency for Fundamental Rights, Facial recognition technology: fundamental rights considerations in the context of law enforcement, Wien 2019, S. 24.

68 Schweizerische Strafprozessordnung vom 5. Oktober 2007 (StPO; SR 312.0).

69 Dazu ausführlich SIMMLER/CANOVA (Fn. 5), S. 18 ff. Immerhin erwähnt § 32c Polizeigesetz des Kantons Zürich vom 23. April 2007 (PolG-ZH; LS 550.1) die offene oder verdeckte Videoüberwachung dergestalt, dass Personen damit identifiziert werden können, jedoch stellt diese Norm (gem. SIMMLER/CANOVA) keine ausreichende gesetzliche Grundlage dar; ebenso auch Art. 45b Polizeigesetz des Kantons Basel-Landschaft vom 28. November 1996 (PolG-BL; SGS 700) nicht.

des Kantons Zürich[70], die durch Art. 102 und 103 AIG[71] abgelöst wurde. Als Konkretisierung ist ausserdem Art. 45 VEV[72] zur automatisierten Grenzkontrolle zu nennen und Art. 54-62 VEV als Grundlage und Rahmenbedingungen für die Zulässigkeit des Einsatzes eines Gesichtserkennungssystems durch die Grenzbehörden.

b) Versammlungs- und Meinungsfreiheit

30 Der Einsatz von maschineller Gesichtserkennung im öffentlichen Raum kann weitere Grundrechte berühren.[73] Zu bedenken ist insbesondere die potenzielle Abschreckungswirkung (sog. *chilling effect*) auf die Grundrechtsausübung.[74] Würde der öffentliche Raum z. B. während einer Demonstration mittels Gesichtserkennung überwacht, könnte dies dazu führen, dass Personen von der Teilnahme an einer Kundgebung zurückschrecken, weil sie negative Konsequenzen – allein aufgrund einer Teilnahme an einer Demonstration – befürchten. Damit würde die Ausübung der Meinungs- und Versammlungsfreiheit (Art. 16 Abs. 1 bzw. Art. 22 Abs. 1 BV) tangiert. Der Einsatz von maschineller Gesichtserkennung im öffentlichen Raum könnte mithin zu einer mittelbaren Grundrechtsbeeinträchtigung führen.[75]

c) Diskriminierungsverbot

31 Beim Einsatz von Gesichtserkennung gibt es sog. *false positives,* also Resultate, die fälschlicherweise eine Übereinstimmung anzeigen, wo keine vorliegt, und sog. *false negatives,* indem keine Übereinstimmung angezeigt wird, obwohl eine vorliegt. Bei einer hohen überprüften Personenzahl führt auch eine kleine *False-positive*-Rate zur falschen Meldung einer Übereinstimmung bei zahlreichen Personen.[76] Eine Konsequenz von *false positives* könnte die vermehrte Kontrolle bzw. Überprüfung dieser Personen sein oder gar eine ungerechtfertigte Festnahme; eine Konsequenz von *false negatives* das Entstehen von Sicherheitsproblemen.[77]

32 Die Auswirkungen falscher Identifizierungen zeigen sich umso eindringlicher, wenn die Fehlerrate bei bestimmten Personengruppen höher ausfällt als bei anderen, insbesondere, wenn an ein verpöntes Merkmal im Sinne des Diskriminierungsverbots nach Art. 8 Abs. 2 BV angeknüpft wird. Dies kann eintreffen, wenn Personen, die in den Datenbanken, mit denen die Gesichtserkennungssoftware trainiert wird, untervertreten sind, was vor allem auf dunkelhäutige/nicht kaukasische Personen, Frauen und jüngere Menschen zutrifft.[78] Durch die geringere Vertretung in den Trainingsdaten erkennt die Software diese Personen schlechter.[79] Es stellt sich mithin die Frage, ob diesfalls der Einsatz maschineller Gesichtserkennung überhaupt als geeignet (i. S. d. Verhältnismässigkeitsgrundsatzes) eingestuft werden kann.

IV. Moratorium statt Verbot

33 Der EU-KI-Verordnungsentwurf sieht ein Verbot jeglicher KI-Software zur Erfassung biometrischer Daten vor, allerdings mit Erlaubnisvorbehalt.[80] Die EU-Kommission verfolgt damit einen risikobasierten Ansatz, der für unterschiedliche KI-Systeme unterschiedliche Abstufungen enthält.[81] Gesichtserkennungssoftware wird gem. Art. 6 Abs. 2 EU-KI-Verordnungsentwurf i. V. m. Nr. 1 des Anhangs III EU-KI-Verordnungsvorschlag als Hoch-Risiko-KI kategorisiert, da mit ihr besondere Gefahren für die Sicherheit, die Grundrechte und die Gesellschaft als Ganzes einhergehen. Im öffentlichen Raum soll das Erfassen biometrischer Daten in Echtzeit deshalb grundsätzlich verboten werden, wobei gewisse Ausnahmen vorgesehen sind. Solche sollen bspw. im Polizeirecht greifen, wenn es um das Auffinden vermisster Kinder oder von Schwerverbrecherinnen und Schwerverbrechern geht

70 Verordnung über den Einsatz eines biometrischen Gesichtserkennungssystems am Flughafen Zürich vom 8. Dezember 2004 (LS 551.113).

71 Bundesgesetz über die Ausländerinnen und Ausländer und über die Integration vom 16. Dezember 2005 (AIG; SR 142.20).

72 Verordnung über die Einreise und die Visumerteilung vom 15. August 2018 (VEV; SR 142.204).

73 Siehe eingehend MÜLLER (Fn. 36), S. 97 ff.

74 Siehe z. B. BGE 143 I 147 E. 3.3.

75 FRA (Fn. 67), S. 29 f.; MÜLLER (Fn. 36), S. 152.

76 Bei einer Personenzahl von 100'000 führt eine *False-positive*-Rate von bloss 1% dennoch zu 1'000 *false positives*.

77 Wobei zu betonen ist, dass in der Schweiz die Ergebnisse der Software noch durch Menschen überprüft werden – hier ist insb. wichtig, die zuständigen Behörden für diese Thematik zu sensibilisieren, vgl. NADJA BRAUN BINDER et al., Künstliche Intelligenz: Handlungsbedarf im Schweizer Recht, Jusletter vom 28. Juni 2021; ferner PATRICK GROTHER / MEI NGAN / KAYEE HANAOKA, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, NISTIR 8280 vom 19. Dezember 2019.

78 MAËLIG JACQUET / LIONEL GROSSRIEDER, Enjeux et perspectives de la reconnaissance faciale en sciences criminelles, Criminologie 54(1)/2021 S. 135 ff., Rn. 47; FRA (Fn. 67), S. 27.

79 BRENDAN F. KLARE et al., Face recognition performance: role of demographic information, IEEE Transactions on Information Forensics and Security 7/2012, S. 1789 und 1800. Ausführlich zur Diskriminierung vgl. auch ALMA KOLLECK / CARSTEN ORWAT, Mögliche Diskriminierung durch algorithmische Entscheidungssysteme und maschinelles Lernen – ein Überblick, TAB 10/2020, S. 53 ff.; GROTHER/NGAN/HANAOKA (Fn. 77).

80 Siehe m. w. H. GERALD SPINDLER, Der Vorschlag der EU-Kommission für eine Verordnung zur Regulierung der Künstlichen Intelligenz, IT und Software – Aufsätze 6/2021, S. 365; DIETER KUGELMANN, EU-Vorschlag zu Künstlicher Intelligenz muss aus Datenschutz-Perspektive durchleuchtet werden, Datenschutz und Datensicherheit 7/2021, S. 433; MARIO MARTINI, Gesichtserkennung im Spannungsfeld zwischen Freiheit und Sicherheit, in: Pfeffer (Hrsg.), Schriftenreihe der Forschungsstelle Europäisches und Deutsches Sicherheitsrecht (FEDS), Band 4, Göttingen 2022, S. 65 ff. Einzelne EU-Parlaments-Abgeordnete fordern dagegen ein Moratorium, siehe ALEXANDER FANTA, EU-Abgeordnete fordern Auszeit für Gesichtserkennung netzpolitik vom 30. Juni 2021.

81 Ausführungen zur EU-Regulierung z. B. von MARTIN SCHALLBRUCH, EU-Regulierung der Künstlichen Intelligenz, Datenschutz und Datensicherheit 7/2021, S. 441.

(Art. 5 Abs. 1 lit. d Ziff. i-iii EU-KI-Verordnungsvorschlag).[82] Dies allerdings nur, wenn strikte Sicherungsauflagen eingehalten werden, eine vorgängige Genehmigung erteilt wurde und eine unabhängige Kontrollinstanz existiert (Art. 5 Abs. 2 und 3 EU-KI-Verordnungsvorschlag). Fraglich ist, ob mit einem solchen Verbot mit Erlaubnisvorbehalt Massenüberwachung tatsächlich verhindert werden kann.[83]

34 Die Herangehensweise der EU-Kommission stellt für die Schweiz ohnehin kein taugliches Vorbild dar. Zum einen steht in der Schweiz die Schaffung eines allgemeinem KI-Gesetzes – zurecht – nicht auf der politischen Agenda.[84] Zum anderen liesse sich eine solche zentrale Regelung nur schwer mit der Kompetenzaufteilung zwischen Bund und Kantonen vereinbaren. Dem Bund kommt insbesondere im Bereich der Polizeiorganisation keine umfassende Kompetenz zu.

35 Gleichwohl ist festzuhalten, dass in der Schweiz bislang eine gesetzliche Grundlage für den Einsatz von maschineller Gesichtserkennung im öffentlichen Raum fehlt,[85] was angesichts der Grundrechtsrelevanz des Themas durchaus kritisch zu beurteilen ist. Vor diesem Hintergrund fordern denn auch verschiedene Akteurinnen und Akteure ein grundsätzliches Verbot bzw. ein Moratorium, vor allem für den Einsatz von Gesichtserkennungstechnologie zwecks Massenüberwachung.[86]

Aus rechtlicher Sicht ist ein explizites, durch den Gesetzgeber zu verankerndes Verbot, zumindest für den staatlichen Einsatz von maschineller Gesichtserkennung, nicht notwendig, weil ein solcher Einsatz ohnehin eine entsprechende formell-gesetzliche Grundlage und damit ein Tätigwerden des Gesetzgebers voraussetzt. Mit Blick auf Private erscheint ein generelles Verbot ebenfalls nicht unbedingt zielführend, da damit die grundrechtskonforme Entwicklung von Gesichtserkennungssystemen verhindert werden könnte. Ein Moratorium erscheint dagegen sinnvoll, da damit eine gesellschaftliche und politische Debatte angestossen und darauf hingewirkt werden kann, dass der Einsatz von Gesichtserkennungssoftware mit einem genügenden Grundrechtsschutz einhergeht. 36

V. Fazit

Die Schaffung eines einzelfallweise zulässigen Einsatzes maschineller Gesichtserkennung, wie im EU-KI-Verordnungsentwurf vorgesehen, kann zum Entstehen juristischer Graubereiche führen. Für die Schweiz wird als sinnvoller erachtet, mithilfe eines Moratoriums für maschinelle Gesichtserkennung im öffentlichen Raum einen breiten gesetzgeberischen und gesellschaftspolitischen Diskurs anzustossen und damit nach Möglichkeiten grundrechtskonformer Lösungen zu suchen. 37

82 Siehe dazu bspw. CHRISTOPH HERWARTZ / MORITZ KOCH, Soll Gesichtserkennung zur Verbrecherjagd erlaubt sein? Streit um die neuen KI-Regeln der EU, Handelsblatt vom 22. April 2021.

83 M. w. H. SPINDLER (Fn. 81), S. 365; KUGELMANN (Fn. 81), S. 433; FANTA (Fn. 81); MATTHIAS REICHE, EU will Künstliche Intelligenz zähmen, Tagesschau vom 21. April 2021.

84 Siehe etwa FLORENT THOUVENIN et al., Positionspapier vom 10. November 2021 «Ein Rechtsrahmen für Künstliche Intelligenz».

85 Bezüglich der Polizeiarbeit haben dies SIMMLER/CANOVA (Fn. 5), S. 17 ff., bereits ausführlich erörtert. Gleichzeitig halten sie jedoch fest, dass die Polizei trotz Fehlen einer gesetzlichen Grundlage gewisse Technologien bereits anwendet.

86 Siehe FLORENT THOUVENIN et al. (Fn. 84) sowie im vorliegenden Beitrag Fn. 3 und 4.

Résumé

L'utilisation de la reconnaissance faciale automatique dans l'espace public comporte le risque d'une surveillance de masse de la société. Si des données biométriques identifiant clairement un individu sont utilisées, il s'agit, selon la nouvelle loi sur la protection des données, d'un traitement de données personnelles sensibles. En Suisse, la reconnaissance faciale automatique n'est guère encadrée par la réglementation. Il est pourtant urgent de réfléchir à cette question. Cela résulte, d'une part, de l'importance de cette question en termes de droits fondamentaux et, d'autre part, de la volonté de certaines organisations de la société civile d'interdire une telle utilisation de ces données. La réglementation européenne prévue en matière d'intelligence artificielle, qui inclut la reconnaissance faciale, devrait également être prise en compte dans les réflexions. Dans ce contexte, le présent article donne un aperçu des questions juridiques qui se posent s'agissant de la reconnaissance faciale automatique dans l'espace public et se penche sur la question de la nécessité d'une interdiction ou d'un moratoire.