Monika Simmler / Giulia Canova*

Gesichtserkennungstechnologie: Die «smarte» Polizeiarbeit auf dem rechtlichen Prüfstand

Die Gesichtserkennungstechnologie gewinnt wie andere «smarte» Technologien in der Polizeiarbeit an Bedeutung. Der Beitrag überprüft die Rechtmässigkeit ihres Einsatzes in der Prävention und Strafverfolgung. Die Analyse zeigt, dass sich de lege lata in der Schweiz weder im Polizei- noch im Strafprozessrecht ausreichende Rechtsgrundlagen finden. Da sich die Technologie dennoch verbreitet, hat sich der Gesetzgeber ihrer Regulierung anzunehmen. Dabei sind dem Einsatz der «Face Recognition» klare Grenzen zu setzen.

La reconnaissance faciale fait partie des technologies « intelligentes » qui gagnent en importance dans les activités de la police. Le présent article examine la licéité de son utilisation dans la prévention et la poursuite pénale. L'analyse montre que de lege lata, des bases légales font défaut en Suisse, que ce soit dans le droit de la police ou dans celui de la procédure pénale. Étant donné que cette technologie se répand malgré tout, il appartient au législateur de la réguler. Il convient dans ce cadre de fixer des limites claires à la reconnaissance faciale.

Inhalt

I. Einleitung

Zwischen 2017 und 2019 setzte die Polizei in Wales Gesichtserkennungstechnologie ein. Bei 50 Einsätzen wurden etwa 500'000 Gesichter gescannt und automatisch mit einer «Watchlist» von gesuchten Personen abgeglichen.[1] Der Einsatz geschah vorwiegend bei Grossveranstaltungen – u.a. beim Champions-League-Finale in Cardiff 2017.[2] Für Schlagzeilen sorgte nicht nur die Verwendung der Technologie, sondern insbesondere die darauffolgende Prüfung der Zulässigkeit ihres Einsatzes. So beurteilte ein britisches Gericht 2020 das Pilotprojekt der walisischen Polizei aufgrund zu unbestimmter Rechtsgrundlagen für unrechtmässig.[3]

Trotz dieses gerichtlichen Appells an die Rechtsstaatlichkeit sowie anhaltender Berichterstattung über die mangelnde Qualität der «Face Recognition»-Technologie[4] verbreiten sich derartige Anwendungen in der Polizeiarbeit. Das gilt auch für die Schweiz, wo Polizeikorps Gesichtserkennungssoftware bereits beschaffen und testen: Die Kantonspolizei St. Gallen verwendet zur Aufklärung von schweren Straftaten eine Gesichtserkennungssoftware, bei der Bildmaterial von mutmasslichen Täterinnen und Tätern ausgewertet und

* Monika Simmler, Prof. Dr., Assistenzprofessorin für Strafrecht, Strafprozessrecht und Kriminologie, Universität St. Gallen; Giulia Canova, B.A. Law and Economics, wissenschaftliche Assistentin am Kompetenzzentrum für Strafrecht und Kriminologie an der Universität St. Gallen.

[1] Markus Reuter, Gericht erklärt automatisierte Gesichtserkennung in Südwales für illegal; abrufbar unter: https://netzpolitik.org/2020/urteil-gericht-erklaert-automatisierte-gesichtserkennung-in-suedwales-fuer-illegal/ (besucht am 24. August 2021).

[2] Reuter (FN 1).

[3] Barrie Gordon, Automated Facial Recognition in Law Enforcement: The Queen (On Application of Edward Bridges) v The Chief Constable of South Wales Police, Potchefstroom Electronic Law Journal 24/2021, 3 ff.; dazu auch Nadja Braun Binder et al., Künstliche Intelligenz: Handlungsbedarf im Schweizer Recht, Jusletter vom 28. Juni 2021, N 16 ff.

[4] Dazu z.B. Jochen Siegel, Gesichtserkennung versagt in London, in: NZZ vom 8. Juli 2019.

mit Bildern in Polizeidatenbanken abgeglichen wird.[5] Auch die Kantonspolizei Aargau nutzt seit 2021 eine Software, die Fahndungsbilder von mutmasslichen Täterinnen und Tätern analysiert und diese anhand von Bildern in Polizeidatenbanken identifizieren soll.[6] Die Schaffhauser Polizei greift auf ein ähnliches System zurück.[7] Es ist anzunehmen, dass diese Kantone keine Einzelfälle sind bzw. keine Einzelfälle bleiben.

Als bedeutsame technologische Entwicklung kann die Gesichtserkennungstechnologie zweifellos zur Prävention und Aufklärung von Straftaten und dabei insbesondere zu Sicherheits- und Fahndungszwecken eingesetzt werden. Sie bringt kriminalistisch viel Potenzial mit sich, zugleich aber nicht minder grosse rechtsstaatliche Bedenken. Damit wird sie zum Sinnbild dafür, dass das Zeitalter der «intelligenten» Technologie in der Strafrechtspflege und Polizeiarbeit angebrochen ist. Algorithmen und Künstliche Intelligenz (KI) sollen Straftaten vorhersagen, gefährdende Personen identifizieren, Rückfälle prognostizieren oder die polizeiliche Ermittlungsarbeit unterstützen. Sie sollen damit den Weg bereiten zu einer «Smart Criminal Justice».[8]

Der Einsatz avancierter Technologie und insbesondere der automatisierten Gesichtserkennung wirft zahlreiche grundrechtliche, polizeirechtliche, datenschutzrechtliche und strafprozessrechtliche Fragen auf. Der diesbezügliche rechtliche Rahmen ist bis heute weitgehend ungeklärt und – für die Schweiz – rechtswissenschaftlich wenig erörtert.[9] Die Europäische Union (EU) hat sich der Technologie in ihrem kürzlich vielbeachteten Vorschlag für eine Verordnung zur Regulierung von KI (nachfolgend: «EU-KI-Verordnungsvorschlag») explizit angenommen.[10] Ein vergleichbares Projekt findet sich in der Schweiz nicht.

In Anbetracht dieser Ausgangslage möchte sich dieser Beitrag den rechtlichen Grundlagen des polizeilichen Einsatzes von Gesichtserkennungstechnologie annehmen. Nach einer Einordnung der «Face Recognition» als Teil einer sich entfaltenden Smart Criminal Justice (II.) werden zunächst deren Funktionsweise dargestellt und mögliche Anwendungsbereiche skizziert (III.). Anschliessend werden die Rechtmässigkeit ihres Einsatzes überprüft und Varianten der Regulierung diskutiert (IV.). Ein Fazit rundet die Ausführungen ab (V.). Der Beitrag soll damit am Beispiel der Gesichtserkennung auch aufzeigen, wie «smarte» Technik oft unkritisch Eingang in die Polizeiarbeit findet, ohne dass deren «Smartness» effektiv durchdacht und die Rechtmässigkeit des Einsatzes kritisch überprüft wird.

II. Smart Criminal Justice

Im digitalen Zeitalter wird der Einsatz avancierter Technik zum Paradigma, wobei sich Polizeikorps und Strafbehörden davon mehr Effizienz und Effektivität versprechen.[11] Zahlreiche algorithmenbasierte Anwendungen haben bereits Eingang in die Schweizer Polizeiarbeit und Strafrechtspflege gefunden:[12] Verbreitung finden mitunter Methoden des Predictive Policing, die auf Basis historischer Daten Prognosen erstellen. In der Ermittlungsarbeit kommt zur Analyse grosser Datensätze Data Mining zum Zug, d.h., es werden grosse Datenbestände auf Muster, Trends oder Zusammenhänge hin untersucht. Ferner bilden algorithmische Risk Assessment-Instrumente einen wichtigen Bestandteil der psychiatrischen Begutachtung von Beschuldigten in laufenden Strafverfahren sowie von Verurteilten im Justizvollzug. Dieser vermehrte Einsatz von Algorithmen lässt, wie bereits einleitend festgestellt, eine allgemeine Tendenz hin zur Etablierung einer Smart Criminal Justice erkennen (Abbildung 1). Eine solche gründet auf dem Einsatz von Technologie in der Strafrechtspflege auf Basis einer algorithmischen Entscheidungsfindung und der Erhebung, Analyse sowie Verwertung grosser Datenmengen.[13]

Angesichts des rasanten technologischen Fortschritts entwickeln sich immer weitere Anwendungsformen der Smart Criminal Justice. Dazu gehört auch die Gesichtserkennungstechnologie, welche von Sicherheitsbehörden sowohl präventiv als auch repressiv eingesetzt werden kann.[14] Gesichtserkennungstools basieren auf smarten Systemen, d.h. auf intelligenter algorithmischer Analyse sowie der Nutzung grosser Datenmengen. Im Unterschied zu Predictive Policing oder algorithmischen Risk Assessment-Tools ist die Face

[5] Enrico Kampmann, Umstrittene Technologie: Die Kantonspolizei St. Gallen ist eine der ersten in der Schweiz, die Software zur Gesichtserkennung einsetzt, in: Tagblatt vom 25. Mai 2021, 19 ff.

[6] Simone Luchetta, So jagen Schweizer Polizisten mit Gesichtserkennung Verbrecher, in: Tages-Anzeiger vom 17. April 2021, 39 f.

[7] Luchetta (FN 6), 40.

[8] Zu diesem Phänomen ausführlich die Beiträge in: Monika Simmler (Hrsg.), Smart Criminal Justice, Der Einsatz von Algorithmen in der Polizeiarbeit und Strafrechtspflege, Basel 2021.

[9] Rechtswissenschaftliche Beiträge zur Gesichtserkennung finden sich bislang nur vereinzelt, siehe aber z.B. in Bezug auf den zivilrechtlichen Persönlichkeitsschutz Ramona Keist, Gesichtserkennung im zivilrechtlichen Persönlichkeitsschutz, Jusletter vom 20. Mai 2019.

[10] Siehe Art. 5 des Vorschlags vom 21. April 2021 für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für Künstliche Intelligenz und zur Änderung bestimmter Rechtsakte der Union, COM(2021) 206 final, 2021/0106(COD); abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52021PC0206 (besucht am 22. September 2021).

[11] Vgl. Monika Simmler/Simone Brunner, Smart Criminal Justice in der Schweiz – Die Kantone im Bann der Algorithmen?, in: Simmler (FN 8), 9 ff., 9; vgl. Simon Egbert/Matthias Leese, Criminal Futures, Predictive Policing and Everyday Police Work, Oxon und New York 2021, 8.

[12] Für einen Überblick der eingesetzten Anwendungen siehe Monika Simmler/Simone Brunner/Kuno Schedler, Smart Criminal Justice – Eine empirische Studie zum Einsatz von Algorithmen in der Schweizer Polizeiarbeit und Strafrechtspflege, St. Gallen 2020, 13 ff.

[13] Monika Simmler/Giulia Canova, Smart Government in der Strafrechtspflege: Wann ist Smart Criminal Justice «smart»?, in: Simmler (FN 8), 33 ff., 47.

[14] Andreas Kulick, «Höchstpersönliches Merkmal» – Verfassungsrechtliche Maßstäbe der Gesichtserkennung, Neue Zeitschrift für Verwaltungsrecht 22/2020, 1622 ff., 1622.

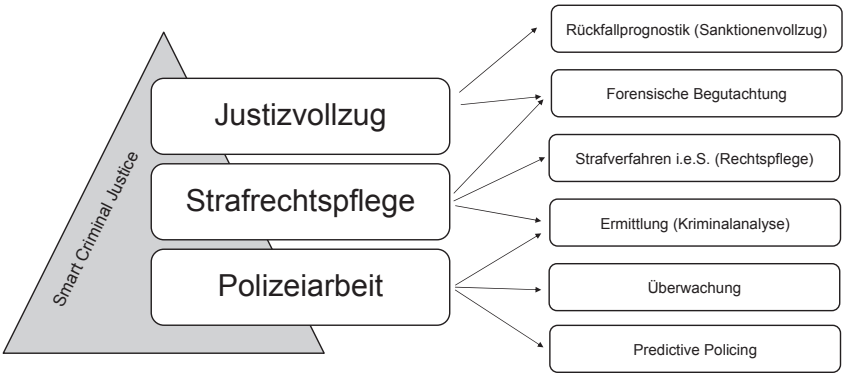

Abbildung 1: Bereiche und Anwendungsfelder der Smart Criminal Justice.

Recognition jedoch wenig erforscht und rechtswissenschaftlich diskutiert.[15]

Die Smart Criminal Justice bringt zahlreiche Herausforderungen mit sich, wie eine Studie bestätigte.[16] Der rechtliche Rahmen des Technikeinsatzes und damit die Gewährleistung der Rechtmässigkeit erwies sich als eine zentrale Herausforderung.[17] Tatsächlich «smarte» Anwendungen müssen aber normative Ansprüche erfüllen wie Effektivität, Transparenz und nicht zuletzt Rechtmässigkeit.[18] Smart ist ein Einsatz von Technologie wie der Gesichtserkennung somit nur, wenn auch dessen Rechtmässigkeit sichergestellt ist.

III. Gesichtserkennungstechnologie in der Polizeiarbeit

1. Gesichtserkennung als biometrisches Verfahren

Im Grundsatz wird unter Gesichtserkennung schlicht die Zuordnung eines Gesichts zu einer bestimmten Person verstanden.[19] Gesichtserkennungstechnologie wird demzufolge eingesetzt, um in Bild- oder Videomaterial Gesichter automatisch zu identifizieren.[20] Gesichtserkennungssysteme können auf zwei verschiedene Arten operieren: Gesichtsverifizierung *(face verification)* oder Gesichtsidentifizierung *(face identification)*.[21] Die Verifizierung erfolgt durch einen 1:1-Vergleich eines aufgenommenen Gesichts mit einer Vorlage des Gesichts, dessen Identität überprüft werden soll. Bei der Identifikation wird hingegen ein aufgenommenes Gesicht mit sämtlichen Vorlagen einer Datenbank abgeglichen (1:n-Vergleich).[22] Die Standardanwendung im polizeilichen Einsatzbereich dürfte ein Abgleich 1:n sein, da die Gesichtserkennung meist genutzt wird, um in einer grossen Menge an Bildmaterial eine bestimmte Person zu suchen. Allerdings kann auch die Verifikation zur Analyse von Beweismaterial massgeblich sein.

Die Gesichtserkennungstechnologie stellt ein klassisches biometrisches Verfahren dar. Biometrische Verfahren bezwecken eine automatisierte Überprüfung der Identität von Menschen anhand biometrischer Merkmale.[23] Biometrische Merkmale sind messbare Körpermerkmale, die eine Identifizierung von Personen ermöglichen, da sie bei jedem Menschen auf einzigartige Weise vorliegen.[24] Biometrische Daten sind also «mit speziellen technischen Verfahren gewonnene personenbezogene Daten […], die eine eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen».[25]

Biometrische Erkennungssysteme funktionieren allesamt nach dem gleichen Grundprinzip.[26] In einem ersten Schritt werden die biometrischen Daten einer Zielperson registriert *(enrolment)*. Dafür wird das biometrische Merkmal mit einem Sensor (z.B. Kamera, Mikrofon, Tastatur) erfasst und ein elektronischer Abdruck mit den biometrischen Rohdaten erstellt. Diese Rohdaten werden dann mittels eines Algorithmus auf ein bestimmtes Muster reduziert und in einen Datensatz umgewandelt *(template)*. Die erzeugten Datensätze werden abgelegt und mit Angaben zur Identität gespeichert.[27] In einer zweiten Phase wird dann mindestens eine weitere Person analysiert, indem dasselbe biometrische Merkmal wiederum mit dem Sensor erfasst und algorithmisch ein «Template» erstellt wird.[28] Dieses wird dann mit den in der Datenbank hinterlegten Templates abgeglichen *(template matching)*.[29]

Automatisierte Gesichtserkennung funktioniert wie die eben beschriebenen Verfahren. Analysiert werden Ge-

[15] Vgl. auch Amélie P. Heldt, Gesichtserkennung: Schlüssel oder Spitzel?, Multimedia und Recht 5/2019, 285 ff., 285, gemäss welcher die Gesichtserkennung zum jetzigen Zeitpunkt gar als unreguliert gilt.

[16] Simmler/Brunner/Schedler (FN 12), 46 ff.

[17] Simmler/Brunner/Schedler (FN 12), 57.

[18] Zu diesen Kriterien siehe Simmler/Canova (FN 13), 48 ff.

[19] Heldt (FN 15), 286.

[20] Vgl. Stan Z. Li/Anil K. Jain, Handbook of Face Recognition, 2. Aufl., London 2011, 1.

[21] Li/Jain (FN 20), 2.

[22] Li/Jain (FN 20), 2 f.

[23] Dominika Blonski, Biometrische Daten als Gegenstand des informationellen Selbstbestimmungsrechts, Diss. Bern 2015 (= Abhandlungen zum schweizerischen Recht, N.F., 816), 6; Astrid Albrecht, Biometrische Verfahren im Spannungsfeld von Authentizität im elektronischen Rechtsverkehr und Persönlichkeitsschutz, Diss. Frankfurt, Baden-Baden 2003 (= Frankfurter Studien zum Datenschutz Bd. 24), 31.

[24] Blonski (FN 23), 6.

[25] So die Definition in Art. 4 Abs. 14 der Datenschutz-Grundverordnung der EU vom 27. April 2016, Verordnung (EU) 2016/679; beinahe identisch auch die Definition der Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017, BBl 2017 6941 ff., 7020.

[26] Albrecht (FN 23), 35.

[27] Zum Ablauf z.B. Blonski (FN 23), 11 f.

[28] Blonksi (FN 23), 12.

[29] Albrecht (FN 23), 35.

sichtszüge als physiologische biometrische Merkmale. In der Registrierungsphase werden die Gesichtszüge von Algorithmen erfasst.[30] In der Regel werden dazu die Abstände zwischen definierten Punkten des Gesichts gemessen (massgebend ist beispielsweise der Abstand zwischen den Wangenknochen oder das Verhältnis zwischen Mund, Nase und Augen).[31] Damit wird eine biometrische Schablone der Gesichtsmerkmale erstellt, wodurch die Gesichtszüge maschinenlesbar werden und mit Schablonen anderer Gesichtsabbildungen verglichen werden können.[32] Die Referenzschablone kann dann u.a. in einer Datenbank abgelegt und mit Informationen über die betreffende Person verknüpft werden.[33] Die Gesichtserkennung i.e.S. erfolgt in einer zweiten Phase durch einen Abgleich von Templates.[34] Für den Abgleich werden die Templates durch einen Algorithmus kombiniert; ergibt sich bei der Kombination eine grosse Ähnlichkeit, die im Bereich einer gewissen Toleranzschwelle liegt, gelten die zugrunde liegenden Gesichter als identisch.[35] Für die Qualität biometrischer Erkennungssysteme sind die Genauigkeit des verwendeten Programms und die verfügbare Datenbasis entscheidend.[36] Die Treffsicherheit der Programme hat sich in den letzten Jahren stetig verbessert, mitunter dank «Deep Learning»-Technologien.[37] Letztlich steht und fällt die Funktionsfähigkeit der Systeme allerdings mit der Qualität und dem Umfang der Datenbasis.

Obwohl die spezifischen technischen Grundlagen der hierzulande bereits eingesetzten bzw. getesteten Gesichtserkennungsanwendungen nicht öffentlich bekannt sind, kann davon ausgegangen werden, dass sie dem eben dargelegten Prinzip folgen. Der Prozess der (polizeilichen) automatisierten Gesichtserkennung gliedert sich also in drei Phasen: Zunächst müssen (1.) die Gesichtsbilder gewonnen werden, die als *Ausgangsdaten* dienen. Ebenso müssen (2.) *Abgleichsdaten* beschaffen werden, d.h. Daten, mit welchen die Ausgangsdaten verglichen werden können. Dies sind bei der Identifikation i.d.R. Datenbanken, bei der Verifikation kann es auch vereinzeltes Bildmaterial sein. Im massgeblichsten Schritt wird schliesslich (3.) die *Gesichtserkennung i.e.S.* bzw. der Abgleich zwischen den beiden Datensätzen vorgenommen. Für diese Analyse müssen zunächst die Ausgangsdaten biometrisch verarbeitet und diese sodann mit den ebenfalls zu Templates verarbeiteten Abgleichsdaten verglichen werden. Die Gesichtserkennung involviert folglich – und das dürfte von juristischer Relevanz sein – zwei verschiedene Datensätze sowie mehrere (biometrische) Datenbearbeitungsschritte.

2. Einsatzbereiche

In der Polizeiarbeit bieten sich vielfältige Anwendungsmöglichkeiten für die Gesichtserkennungstechnologie. Die Differenzierung der Einsatzbereiche ist wesentlich für die rechtliche Würdigung. Nachfolgend werden die Bereiche skizziert, die aufgrund des polizeirechtlich vorgesehenen Aufgabenkatalogs im Fokus stehen. Die Gesichtserkennungstechnologie kann entweder (1.) zwecks allgemeiner Überwachung, d.h. zur Prävention oder zum Zwecke der Erkennung von Straftaten erfolgen. Ferner kann sie (2.) der konkreten Überwachung dienen, d.h. bereits zur spezifischen Gefahrenabwehr oder bei polizeilichen Vorermittlungen. Bei diesen beiden ersten Einsatzbereichen handelt es sich um Überwachungsmassnahmen im präventiven, dem Polizeirecht unterstehenden Bereich. Die Gesichtserkennung kann aber auch strafprozessual eingesetzt werden. Dann dient sie (3.) der Ermittlung im Strafverfahren bzw. der Aufklärung von Straftaten.

2.1 Allgemeine Überwachung

In öffentlich zugänglichen Räumen, die von ihrer Zweckbestimmung her einem unbestimmten Personenkreis zur Benutzung offenstehen,[38] ist die Videoüberwachung bereits alltäglich geworden.[39] So werden Parkanlagen, Bahnhöfe, Einkaufszentren, Sportstadien oder Plätze vielerorts videoüberwacht. Die Infrastruktur zur Überwachung ist dabei entweder stationär installiert oder besteht aus mobilen Überwachungsanlagen (z.B. in Fahrzeugen oder Drohnen).[40] Ist die Videoüberwachung für Betroffene erkennbar (z.B. aufgrund von Hinweistafeln), gilt sie als offene Überwachung, ansonsten erfolgt sie verdeckt.[41]

Die Videoüberwachung dient Sicherheitszwecken, um beispielsweise Einsätze von Personal zu steuern, Personen- und Verkehrsströme zu überwachen oder Straftaten durch Abschreckung zu verhindern.[42] Insofern dient diese Art der Videoüberwachung einerseits dem präventiven Schutz von Polizeigütern, andererseits dem Erkennen (und ggf. in der Folge dem Aufklären) von Straftaten. Sie wird also durch eine abstrakte Gefahr gerechtfertigt.[43] Im Unterschied zu einer konkreten Gefahr

[30] Keist (FN 9), N 10.
[31] Nina Elisabeth Herbort, Digitale Bildnisse, Objektbezogene Interessengeflechte zwischen Urhebern, Abgebildeten und Nutzern in der digital-vernetzten Kommunikation, Diss. Berlin 2016, Tübingen 2017 (= Internet und Gesellschaft 8), 284 f.
[32] Herbort (FN 31), 284.
[33] Alexander Rossnagel, Handbuch Datenschutzrecht, Die neuen Grundlagen für Wirtschaft und Verwaltung, München 2003, Kap. 9.6, Rn. 6; Herbort (FN 31), 285.
[34] Blonski (FN 23), 25; Keist (FN 9), N 11.
[35] Herbort (FN 31), 285.
[36] Herbort (FN 31), 285.
[37] Dazu Bruce Ho, Deep Learning: Image and Video Recognition; abrufbar unter: http://bigr.io/wp-content/uploads/2017/09/BigR.io-Deep-Learning-Image-and-Video-Recognition.pdf (besucht am 23. September 2021).
[38] Zur Definition des öffentlichen Raums Lucien Müller, Videoüberwachung in öffentlich zugänglichen Räumen – insbesondere zur Verhütung und Ahndung von Straftaten, Diss. St. Gallen, Zürich 2011, 8 ff.; Jürg Marcel Tiefenthal, Kantonales Polizeirecht der Schweiz, Zürich 2018, § 18 N 4; BSK StPO II-Eugster/Katzenstein, Art. 282 N 5.
[39] Müller (FN 38), 1; Gerrit Hornung/Stephan Schindler, Das biometrische Auge der Polizei, Zeitschrift für Datenschutz 5/2017, 203 ff., 203.
[40] Tiefenthal, Polizeirecht (FN 38), § 21 N 2.
[41] Müller (FN 38), 24; Tiefenthal, Polizeirecht (FN 38), § 21 N 2.
[42] Vgl. Müller (FN 38), 1.
[43] Vgl. Tiefenthal, Polizeirecht (FN 38), § 21 N 3.

besteht die Wahrscheinlichkeit eines Schadeneintrittes bloss hypothetisch und knüpft an eine typische Gefährdungslage an.[44] Als *allgemeine Überwachung* kann diese Art der Überwachung bezeichnet werden, da sie weder an das Vorliegen eines Tatverdachts anknüpft noch der Überwachung spezifischer Vorkommnisse oder einzelner Personen dient.

Bestehende Videoüberwachungsinfrastruktur in öffentlich zugänglichen Räumen kann mit Gesichtserkennungstechnologie ergänzt werden.[45] Damit können sämtliche Gesichter der Personen, welche den von der Kamera erfassten Bereich passieren, biometrisch erfasst werden. Die erfassten Gesichter können dann mit einer Datenbank abgeglichen werden.[46] In Deutschland wurde die biometrische Gesichtserkennung mittels allgemeiner Videoüberwachung am Bahnhof Berlin Südkreuz getestet.[47] Dafür wurde die Technologie in die bestehende Videoüberwachungsinfrastruktur eingebunden. Alle Personen, welche das Aufnahmefeld der Videokamera passierten, wurden aufgenommen und deren Templates erfasst. Die algorithmisch verarbeiteten Daten konnten in der Folge mit einer Datenbank abgeglichen werden, um Personen zu identifizieren.[48] Solche Anwendungen bedingen, dass biometrische Daten sämtlicher Passantinnen und Passanten eines bestimmten Bereiches verarbeitet werden, auch wenn diese dazu nicht konkret Anlass gegeben haben. Der generelle Einsatz von Gesichtserkennung i.V.m. Videoüberwachung stellt daher eine anlasslose und verdachtsunabhängige Massnahme mit grosser Streubreite dar, die vielfältige Möglichkeiten zur Auswertung der Daten bietet.[49] Treffermeldungen verschiedener Videokameras im öffentlichen Raum können zudem miteinander verknüpft werden, was die Erstellung von Bewegungsprofilen erlaubt und Rückschlüsse auf das Verhalten von Individuen ermöglicht.[50] Während es sich in Deutschland um einen Test handelte, kommen intelligente Kameras mit Gesichtserkennungsfunktion zur Überwachung des öffentlichen Raumes in den USA und Grossbritannien bereits standardmässig zum Einsatz.[51]

2.2 Konkrete Überwachung

Der Einsatz von Gesichtserkennungstechnologie kann auch als sicherheitspolizeiliche Massnahme zur konkreten Gefahrenabwehr sowie zwecks polizeilicher Vorermittlungen erfolgen. So wird Gesichtserkennungstechnologie bereits heute – wenn auch bis jetzt soweit ersichtlich nicht in der Schweiz – von der Polizei bei Grossveranstaltungen eingesetzt. Wie bereits einleitend geschildert, hatte von ihr z.B. die walisische Polizei bei etwa 50 Grossveranstaltungen Gebrauch gemacht.[52] Dazu wurden an bestimmten Orten Videokameras aufgestellt, die Bilder der Gesichter aller passierender Personen erstellten. Die Templates wurden in Echtzeit extrahiert und dann mit den biometrischen Informationen von Personen auf einer «Watchlist» abgeglichen.[53] Die Liste enthielt Bilder von Personen, die zur Verhaftung ausgeschrieben waren, weil sie im Verdacht standen, eine Straftat begangen zu haben, oder weil sie als gefährlich eingestuft worden waren.[54]

Auch in der Schweiz könnten bei Grossveranstaltungen Videokameras installiert werden, die mit Gesichtserkennungstechnologie ausgestattet sind. Bei Sportveranstaltungen könnten sie beispielsweise der Eingangskontrolle dienen, um in Polizeidatenbanken registrierte Hooligans aufzuspüren oder Personen mit Stadionverbot zu identifizieren.[55] Aber auch bei Demonstrationen wird auf Gesichtserkennungstechnologie zurückgegriffen. Bereits in mehreren Ländern – darunter in Deutschland und Österreich – wurde Gesichtserkennungssoftware im Nachgang von Demonstrationen eingesetzt, um mutmassliche Täterinnen und Täter auszuforschen.[56] Ein Einsatz bei Demonstrationen wäre sodann präventiv möglich, wobei schon während der Versammlung das Geschehen überwacht und einzelne Personen beobachtet und ggf. sogleich identifiziert werden können.

In Kombination mit der Videoüberwachung kann die Gesichtserkennungstechnologie bei Grossveranstaltungen oder Demonstrationen also der Abwehr von konkreten Gefahren dienen. Im Unterschied zur abstrakten Gefahrlage liegt bei einer konkreten Gefahr ein Geschehen vor, welches mit einer gewissen hinrei-

[44] Müller (FN 38), 26, FN 156; Rainer J. Schweizer/Patrick Sutter/Nina Widmer, Grundbegriffe, in: Schweizer (Hrsg.), Sicherheits- und Ordnungsrecht des Bundes, Teil 1, Allgemeiner Teil, Basel 2008, N 27; Hans Reinhard, Allgemeines Polizeirecht, Aufgaben, Grundsätze und Handlungen, Diss. Bern 1993, 111 f.; vgl. dazu auch BGE 136 I 87 E. 8.3. (114 ff.), wonach sich die Videoüberwachung auf bestimmte Bereiche, in denen z.B. Gefährdungen oder die Begehung von Straftaten ernsthaft zu erwarten sind, beschränken muss.

[45] Vgl. Hornung/Schindler (FN 39), 204.

[46] Zur Funktionsweise vorne Kap. III.1.

[47] Miriam Salzmann/Stephan Schindler, Polizeiliche Gesichtserkennung in Deutschland, Zeitschrift für Datenschutzrecht-Aktuell 18/2018, 06344.

[48] Salzmann/Schindler (FN 47), 06344.

[49] Hornung/Schindler (FN 39), 207 f.

[50] Salzmann/Schindler (FN 47), 06344.

[51] Vgl. Heldt (FN 15), 285 f.

[52] Siehe dazu das in FN 3 bereits erwähnte Urteil R (Bridges) v CCSWP and SSHD, C1/2019/2670, [2020] EWCA Civ 1058, N 11.

[53] Urteil R (Bridges) v CCSWP and SSHD, C1/2019/2670, [2020] EWCA Civ 1058, N 12.

[54] Urteil R (Bridges) v CCSWP and SSHD, C1/2019/2670, [2020] EWCA Civ 1058, N 13.

[55] So tat dies z.B. ein dänischer Fussballklub, siehe SRF vom 1. September 2019, «Heute im Stadion, morgen überall?»; abrufbar unter: https://www.srf.ch/news/panorama/automatische-gesichtserkennung-heute-im-stadion-morgen-ueberall (besucht am 31. August 2021).

[56] So in Österreich nach Demonstrationen in Wien-Favoriten im Sommer 2020, dazu Der Standard vom 15. September 2020; abrufbar unter: https://www.derstandard.de/story/2000119996329/polizei-nutzt-neue-gesichtserkennung-um-demonstranten-zu-identifizieren (besucht am 24. Juli 2021); in Deutschland nach Ausschreitungen am G-20-Gipfel in Hamburg im Sommer 2017, dazu Salzmann/Schindler (FN 47), 06344; und in den USA bei Black-Lives-Matter-Kundgebungen im Herbst 2020 oder bei der Stürmung des Kapitols im Januar 2021, dazu Adelaide Bragias/Kelly Hine/Robert Fleet, «Only in our best interest, right?» Public perceptions of police use of facial recognition technology, Police Practice and Research 2021, 1637 ff., 1638.

chenden Wahrscheinlichkeit zu einem Schaden für ein polizeiliches Schutzgut führt.[57] Die Überwachung und Identifikation fungiert gewissermassen als «verlängertes Auge» der Polizei, um Personenströme zu überwachen, bei Unfällen, Tumulten oder Gewaltakten direkt reagieren zu können und Straftaten unmittelbar zu entdecken.[58] Es handelt sich dabei insofern um eine *konkrete Überwachung*, als dass sie auf Störungen, Störerinnen und Störer gerichtet ist.[59] Allerdings werden davon i.d.R. auch unbeteiligte Dritte in ihren Rechten tangiert.

Zur konkreten Überwachung gehört ebenfalls die polizeiliche Vorermittlungstätigkeit. Vorermittlungen sind Massnahmen der Polizei, welche auf Verdachtsbegründung gerichtet sind oder auf vagen Anhaltspunkten, kriminalistischen Erfahrungswerten oder auf einer blossen Vermutung oder Hypothese gründen, die für die Eröffnung eines strafprozessualen Vorverfahrens oder polizeilichen Ermittlungsverfahrens nicht genügen.[60] Die Polizei nimmt Vorermittlungen primär im sogenannten kriminalitätsgeneigten Umfeld (z.B. Drogenhandel, Rocker- oder Hooliganszene) vor.[61] Meist werden dafür auf einer breiten Basis Informationen über bestimmte Personen beschafft und ausgewertet, bei denen entfernt eine Verbindung zu einer konkreten Straftat vermutet wird.[62] Diese Informationsbeschaffung und -auswertung würde sich für einen Einsatz von Gesichtserkennungstechnologie anbieten. So könnten z.B. Personen verdeckt beobachtet oder polizeilich observiert und unter der Verwendung von Gesichtserkennungssystemen direkt identifiziert werden. Der Erkennungsprozess könnte u.a. durch eine von einem Ermittler getragene Bodycam automatisiert erfolgen. Auch beim Einsatz von Gesichtserkennungssoftware im Rahmen von Vorermittlungen handelt es sich um Massnahmen der konkreten Überwachung, die von Überwachungen bzw. Identifikationen im Rahmen der Strafverfolgung abzugrenzen sind.

2.3 Strafverfolgung

Technische Überwachungsmassnahmen dienen der Polizei nicht nur zur Gefahrenabwehr, sondern insbesondere zur Verfolgung von Straftaten.[63] In der Ermittlungsarbeit kann die Gesichtserkennungstechnologie hilfreich sein und es ist auch ausschliesslich dieser Einsatzbereich, in dem die Technologie bis anhin (soweit bekannt) in der Schweiz polizeilich zur Anwendung kommt.[64] Auf Gesichtserkennungssoftware kann im Nachgang zu Straftaten bei der Sichtung von Videomaterial zurückgegriffen werden, um Täterinnen und Täter zu identifizieren. Videoaufzeichnungen des Tatgeschehens können mit ihrer Hilfe durchforstet werden. Die analysierten Gesichter werden mit polizeilichen Datenbanken, insbesondere erkennungsdienstlichen Lichtbildsammlungen,[65] abgeglichen.[66] Die Technologie ermöglicht die Wiederkennung einzelner Personen in einer grossen Datenmenge. Im Vergleich zur herkömmlichen manuellen Sichtung durch Polizeiangehörige kann die automatisierte Gesichtserkennung somit enorme Zeitersparnis bedeuten.[67]

Wird Gesichtserkennungstechnologie wie im bereits erwähnten Beispiel bei Demonstrationen eingesetzt, unterstützt sie einerseits die Identifikation von Personen, andererseits kann sie auch der Rekonstruktion des Verhaltens dienen. Dafür kann grossflächig Bildmaterial von Überwachungskameras oder aus anderen Quellen (z.B. Aufnahmen aus sozialen Medien) gesammelt und mit Datenbanken abgeglichen werden. Zur Veranschaulichung kann der Einsatz entsprechender Software nach dem G-20-Gipfel in Hamburg dienen: Nach den Protesten und Ausschreitungen sammelte die Polizei 100 Terabyte an Bild- und Videoaufnahmen, die aus polizeieigenen oder polizeifremden Quellen (Überwachungskameras an Bahnhöfen, Aufnahmen aus dem Internet oder von Medien sowie Privatpersonen zur Verfügung gestellte Bild- und Videoaufnahmen) stammten.[68] Die Software erstellte dann biometrische Templates und hinterlegte diese in einer Datenbank, um sie dann mit Templates bereits identifizierter Personen automatisiert abzugleichen.[69] Insbesondere konnten so Erkenntnisse über das Vor- und Nachtatverhalten erlangt oder identifizierten Personen weitere Straftaten zugeordnet werden.[70]

[57] Vgl. Reinhard (FN 44), 110 m.w.N.; Schweizer/Sutter/Widmer (FN 44), 73; Müller (FN 38), 26, FN 150.

[58] Müller (FN 38), 23, 26; vgl. Marianne Gras, Die Videoüberwachung öffentlicher Räume, in: Jehle/Schöch (Hrsg.), Angewandte Kriminologie zwischen Freiheit und Sicherheit (= Neue Kriminologische Schriftenreihe 109), Mönchengladbach 2004, 245.

[59] Dies entspricht grundsätzlich dem im Polizeirecht etablierten Störerprinzip, gemäss dem sich verhältnismässige polizeiliche Massnahmen nur gegen die Verursacher der Störung zu richten haben; dazu anstatt vieler Daniel Thürer, Das Störerprinzip im Polizeirecht, ZSR I 4/1983, 463 ff.; Pierre Tschannen/Ulrich Zimmerli/Markus Müller, Allgemeines Verwaltungsrecht, 4. Aufl., Bern 2014, § 56 N 28 ff., oder § 18 des PolG ZH. Allerdings gibt es Ausnahmen von diesem Prinzip, namentlich in Fällen polizeilichen Notstands oder bei Vorliegen eines Gesetzesvorbehalts; siehe z.B. Tiefenthal, Polizeirecht (FN 38), § 5 N 38 f.

[60] BGE 140 I 353 E. 6.1 (365); Tobias Jaag/Sven Zimmerlin, Die Polizei zwischen Gefahrenabwehr und Ermittlung von Straftaten, in: Jositsch/Schwarzenegger/Wohlers (Hrsg.), Festschrift für Andreas Donatsch, Schulthess Zürich/Basel/Genf 2017, 406; BSK StPO II-Rhyner, Art. 306 N 8.

[61] Jaag/Zimmerlin (FN 60), 407.

[62] BSK StPO II-Rhyner, Art. 306 N 9.

[63] Müller (FN 38), 28; vgl. Reinhard (FN 44), 132 ff.

[64] Luchetta (FN 6), 39.

[65] Hornung/Schindler (FN 39), 207.

[66] Luchetta (FN 6), 39.

[67] Hornung/Schindler (FN 39), 206 f.

[68] Salzmann/Schindler (FN 47), 06344

[69] Prüfbericht des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit, Datenschutzrechtliche Prüfung des Einsatzes einer Gesichtserkennungssoftware zur Aufklärung von Straftaten im Zusammenhang mit dem G20-Gipfel durch die Polizei Hamburg; abrufbar unter: https://datenschutz-hamburg.de/assets/pdf/Pruefbericht_Gesichtserkennungssoftware.pdf (besucht am 24. August 2021), 2.

[70] Prüfbericht des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (FN 69), 6 f.

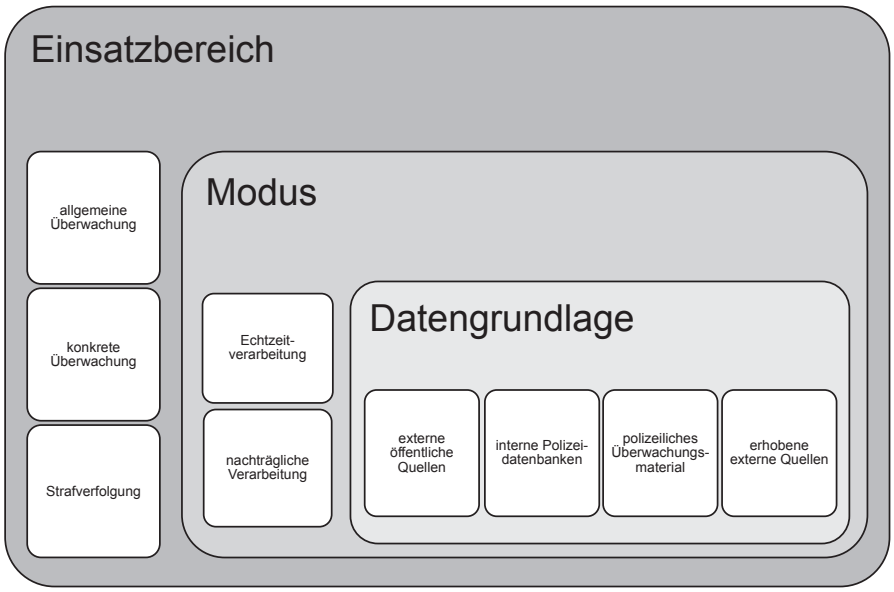

Abbildung 2: Varianten des polizeilichen Einsatzes der Gesichtserkennungstechnologie.

Die Gesichtserkennung kann ferner zur gezielten Fahndung eingesetzt werden. Dazu werden Überwachungssysteme mit einer Fahndungsdatenbank und einem Gesichtserkennungssystem verbunden.[71] Die Gesichter der erfassten Personen können in Echtzeit mit den Gesichtern der Fahndungsdatenbank abgeglichen werden.[72] Sowohl bei der Kriminalanalyse respektive Ermittlungsarbeit i.e.S. als auch bei strafprozessualen Fahndungen handelt es sich um Massnahmen der *Strafverfolgung*. Anders als bei den zuvor definierten Bereichen diente der Einsatz von Gesichtserkennungstechnologie hier also der Aufklärung bereits erfolgter Straftaten und damit repressiven Zwecken.

3. Datengrundlage und Modus

Für die rechtliche Einordnung der Gesichtserkennung ist nicht nur deren Einsatzbereich ausschlaggebend. Auch der Modus der Analyse und die Daten, mit welchen das zu analysierende Gesicht abgeglichen werden, sind entscheidend. Wie der Datenabgleich vonstattengeht und auf welchen Daten die Analyse basiert, entscheidet schliesslich – neben dem ihr zugrunde liegenden Zweck – über die Intensität der mit der Gesichtserkennung einhergehenden Eingriffe in die Freiheit der betroffenen Personen.

Wie dargelegt erfolgt die Gesichtserkennung stets nach demselben Grundprinzip. In einem ersten Schritt setzt sie eine bildtechnische Aufnahme der zu identifizierenden Personen voraus. In der Regel erfolgt diese Aufnahme über Videokameras, weshalb die Gesichtserkennungstechnologie zumeist an Videoüberwachungssysteme anknüpft. Allerdings kann die Aufnahme auch aus einem einzigen Bild bestehen. Erst in einem zweiten Schritt erfolgt die eigentliche Erkennung durch den Abgleich der Gesichter. Möglich ist ein solcher mit polizeiinternen Datenbanken und polizeilichem Überwachungsmaterial. Ebenfalls denkbar ist ein Datenabgleich mit externen Quellen, die nicht öffentlich zugänglich sind, sondern von den Strafbehörden durch einen separaten Rechtsakt beschafft werden (z.B. durch Rechtshilfe, Edition oder Beschlagnahme). Für die Erstellung der Abgleichsdatenbank kann ferner auf externe, öffentlich zugängliche Quellen *(open source information)* zurückgegriffen werden, z.B. mittels Rückgriff auf Fotos aus dem Internet und Social Media. Die Gesichtserkennungssoftware «Clearview AI» beispielsweise nutzt eine Datenbank mit über drei Milliarden Bildern aus dem Internet.[73] Gemäss einer journalistischen Recherche nutzen mindestens 24 Länder die umstrittene Software.[74] Zu diesem Einsatz befragt, liess die Kantonspolizei Zürich verlauten, dass sie «Clearview AI» institutionell nicht nutze. Es könne jedoch nicht ausgeschlossen werden, dass einzelne Angestellte das Tool privat verwendet hätten.[75]

Neben unterschiedlichen Abgleichsdatenbanken kann auch der Modus des Abgleichs selbst variieren. Wie bei der Videoüberwachung kann zwischen einer Echtzeitanalyse und einer nachträglichen Verarbeitung unterschieden werden. Bei einer «Live-Gesichtserkennung» werden die von den Kameras erfassten Gesichter unmittelbar mit der Abgleichsdatenbank abgeglichen.[76] Demgegenüber erfolgt ein nachträglicher Abgleich nur, falls es sich als notwendig erweist. Der gezielte nachträgliche Abgleich ist daher i.d.R. weniger invasiv als die umfassende Echtzeitverarbeitung.

4. Varianten der polizeilichen Gesichtserkennung

Die Darlegung unterschiedlicher Einsatzbereiche, Modi des Datenabgleichs und Abgleichsdaten bzw. -datenbanken erlaubt es, Varianten der polizeilichen Gesichtserkennung zu differenzieren. Dies ist für die rechtliche

[71] Hornung/Schindler (FN 39), 207.
[72] Hornung/Schindler (FN 39), 207.
[73] Isadora Neroni Rezende, Facial recognition in police hands: Assessing the «Clearview case» from a European perspective, New Journal of European Criminal Law 11/2020, 375 ff., 375.
[74] Ryan Mac/Caroline Haskins/Antonio Pequeño IV, Police In At Least 24 Countries Have Used Clearview AI. Find Out Which Ones Here, in: Buzzfeed News vom 25. August 2021; abrufbar unter: https://www.buzzfeednews.com/article/ryanmac/clearview-ai-international-search-table (besucht am 31. August 2021).
[75] Mac/Haskins/Pequeño IV (FN 74), Tabelle.
[76] Vgl. Hornung/Schindler (FN 39), 207.

Analyse notwendig, unterscheiden sich doch die mit den Varianten einhergehende Intensität der Grundrechtseingriffe sowie die massgeblichen Rechtsgrundlagen *(Abbildung 2)*. Diese Differenzierung ist deshalb bei der nachfolgenden rechtlichen Würdigung zu berücksichtigen.

IV. Rechtmässigkeit der automatisierten Gesichtserkennung

1. Gesichtserkennung als Grundrechtseingriff

Wie bei vielen Smart Criminal Justice-Anwendungen ist der Technikeinsatz nur dann «smart», wenn dessen Rechtmässigkeit sichergestellt ist. Die automatisierte Gesichtserkennung wirft diverse rechtliche Fragen auf. Sie stellt in Kombination mit der ihr regelmässig einher- oder vorausgehenden Videoüberwachung und der Notwendigkeit eines Datenabgleichs potenziell einen dreifachen Eingriff für Betroffene dar: erstens durch das Erlangen der Aufnahme der zu identifizierenden Person *(Gewinnung der Ausgangsdaten)*, zweitens durch die biometrische Analyse des entsprechenden Gesichts und dessen Abgleich *(Datenabgleich)* und drittens durch das Heranziehen einer Datenbank zum Zwecke dieses Abgleichs *(Gewinnung der Abgleichsdaten)*. Mindestens bei der Analyse und dem Datenabgleich, d.h. der eigentlichen Gesichtserkennung, werden biometrische Daten bearbeitet, aber auch die Gewinnung und Verwertung der Ausgangs- und Abgleichsdaten betrifft die Bearbeitung von Personendaten. Die Gesichtserkennungstechnologie ist deshalb zweifellos grundrechtlich relevant.

Die automatisierte Gesichtserkennung ist grundsätzlich eingriffsintensiver als die blosse Videoüberwachung mit anschliessender manueller Sichtung durch einen Menschen. Bei einer manuellen Sichtung werden die biometrischen Merkmale bloss durch einen Menschen von Auge erfasst, nicht jedoch wie bei einer automatisierten Gesichtserkennung zu biometrischen Daten verarbeitet und gespeichert. Da die automatisierte Gesichtserkennung die Gefahr von automatisierten Massenüberwachungen mit sich bringt, birgt sie ferner gesellschaftspolitische «Sprengkraft». Die Einordnung dieses neuen polizeilichen Instruments bedingt eine Auseinandersetzung mit dessen (möglichen) rechtlichen Grundlagen. Dafür ist nach den soeben definierten Elementen des Gesichtserkennungsprozesses zu unterscheiden. Sowohl für die Gewinnung der Ausgangs- und Abgleichsdaten als auch für die Gesichtserkennung i.e.S. bedarf es ausreichender Rechtsgrundlagen, wobei auch hier nach dem infrage stehenden Einsatzbereich zu unterscheiden ist.

Den Ausgangspunkt der Gesichtserkennung bilden die Ausgangsdaten. Dabei kann es sich um eine herkömmliche Fotografie handeln, aber auch um Aufnahmen, die aus einer Videoüberwachung stammen. Sie können ein einzelnes Gesicht betreffen, ebenso aber eine gesamte «Watchlist». Jedenfalls handelt es sich dabei um Personendaten,[77] deren Bearbeitung, namentlich deren Erhebung, Sammlung, Verbreitung, Aufbewahrung oder Weitergabe durch Behörden den mit Art. 13 Abs. 2 BV[78] garantierten Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten tangiert.[79] Das sogenannte Recht auf informationelle Selbstbestimmung umfasst jeden Umgang mit personenbezogenen Daten.[80] Konkretisiert wird Art. 13 Abs. 2 BV wesentlich durch das eidgenössische und die kantonalen Datenschutzgesetze.[81]

Die Gewinnung und Bearbeitung der hier als Ausgangsdaten bezeichneten Personendaten, d.h. zu identifizierende Gesichter (und damit Templates), greift bereits in Grundrechte ein. Noch mehr ist aber die Erhebung der Abgleichsdaten relevant, d.h. i.d.R. der Videoaufzeichnungen, in welchen nach dem Ausgangsgesicht gesucht wird. Es handelt sich dabei unabhängig von der Erhebungsart ebenfalls um einen Grundrechtseingriff. Selbstverständlich ist dieser aber je nach Datensatz und -herkunft ungleich intensiv und betrifft ungleich viele Personen. Bei der Beschlagnahme eines Privatvideos sind nur wenige Personen betroffen, die Rechtfertigung in einem laufenden Strafverfahren wäre somit einfacher. Eine Echtzeit-Überwachung an Grossveranstaltungen betrifft hingegen eine unbestimmte Anzahl Personen, die zumeist nicht als Störer zu qualifizieren sind. Eine Videoüberwachung stellt jedenfalls einen Eingriff in den mit Art. 13 BV garantierten Schutz der Privatsphäre dar.[82] Dies gilt sowohl für die Anfertigung von Aufzeichnungen als auch für die reine Beobachtung durch Kameras.[83]

Für jede Einschränkung von Grundrechten verlangt Art. 36 Abs. 1 BV eine gesetzliche Grundlage. Je schwerer der Grundrechtseingriff wiegt, desto höher sind die Anforderungen an diese. Schwerwiegende Eingriffe bedürfen einer Grundlage in einem Gesetz im formellen Sinn. Sofern die polizeiliche technische Überwachung die Bearbeitung von besonders schützenswerten Personendaten oder die Erstellung von Persönlichkeitsprofilen erlaubt, handelt es sich um einen schweren

[77] Der Begriff umfasst gemäss Art. 3 lit. a des Bundesgesetzes über den Datenschutz (DSG) vom 19. Juni 1992, SR 235,1 alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen.

[78] Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999 (BV), SR 101.

[79] Vgl. BSK BV-Diggelmann, Art. 13 N 32 f.; Rainer Schweizer, St. Galler Kommentar zu Art. 13 BV N 72; Regina Kiener/Walter Kälin/Judith Wyttenbach, Grundrechte, 3. Aufl., Bern 2018, § 14 N 2 und 57, m.w.N.

[80] Schweizer, St. Galler Kommentar zu Art. 13 BV, N 74.

[81] BGE 143 I 254 E. 3.3 (257).

[82] BGE 133 I 77 E. 3.2 (80 f.); Müller (FN 38), 97 ff. und 129; Ivo Schwegler, Datenschutz im Polizeiwesen von Bund und Kantonen, Diss. Bern 2011 (= Abhandlungen zum schweizerischen Recht, N.F., 654), 59, 66; Tiefenthal, Polizeirecht (FN 38), § 21 N 5; Jürg Marcel Tiefenthal, Kantonale Polizeihoheit, Eine systematische Darstellung des kantonalen Polizeirechts anhand des Schaffhauser Polizeigesetzes, Zürich 2016, 367. Ebenfalls tangiert werden können die Bewegungsfreiheit (Art. 10 Abs. 2 BV) und die Versammlungsfreiheit (Art. 22 BV).

[83] Hornung/Schindler (FN 39), 205.

Grundrechtseingriff.[84] Bei der Videoüberwachung zum Zwecke der Gesichtserkennung ist dies notwendigerweise der Fall. Infolgedessen ist sie in einem Gesetz im formellen Sinn vorzusehen.[85] Die Abgleichsdaten liegen aber auch regelmässig in Form einer Datenbank mit Fotos oder bereits gespeicherten Templates vor. Die Beschaffung oder Speicherung entsprechender Daten in einer Datenbank berührt ebenfalls den Schutzbereich von Art. 13 Abs. 2 BV, womit auch dafür eine gesetzliche Grundlage notwendig ist.

Alle weiteren Bearbeitungsschritte des Bildmaterials – wie die eigentliche Analyse der biometrischen Daten mittels der Gesichtserkennungstechnologie sowie die Identifikation der Personen mittels Datenabgleichen – stellen weitere, selbstständige Grundrechtseingriffe dar.[86] Bei der Gesichtserkennung werden biometrische Merkmale zu biometrischen Daten verarbeitet.[87] Biometrische Daten sind aus datenschutzrechtlicher Sicht als besonders schützenswert zu qualifizieren, da sie besonders persönlichkeitsnah sind, die höchstpersönliche Sphäre betreffen und sich für die eindeutige Personenzuordnung eignen.[88] Im revidierten eidgenössischen Datenschutzgesetz (nDSG[89]), das im Jahr 2022 in Kraft treten wird, sind biometrische Daten explizit in der Kategorie der besonders schützenswerten Daten aufgeführt (Art. 5 lit. c Ziff. 4 nDSG). Biometrische Daten ermöglichen u.a. Rückschlüsse auf Rasse oder Gesundheitszustand (vgl. Art. 5 lit. c Ziff. 2 nDSG).[90] Die Gesichtserkennung i.e.S. als Verarbeitungsprozess von besonders schützenswerten Personendaten ist deshalb als schwerer Eingriff in die durch Art. 13 Abs. 2 BV geschützten Rechte zu qualifizieren.[91] Aufgrund der automatisierten Verarbeitung biometrischer Daten wiegt dieser gar schwerer als eine herkömmliche personenbezogene Überwachung. Entsprechend bedarf auch dieses Element der automatisierten Gesichtserkennung klarerweise einer formell-gesetzlichen Grundlage.[92]

Im Ergebnis lässt sich festhalten, dass sowohl die Gewinnung der zu identifizierenden Gesichtsbilder als auch die Gewinnung der Abgleichsdaten einer gesetzlichen Grundlage bedarf, wobei sich die konkreten Anforderungen nach dem zu bearbeitenden Material richten. Bei der Gesichtserkennung i.e.S. handelt es sich aufgrund der Verarbeitung biometrischer Daten immer um einen schweren Grundrechtseingriff, der in einem Gesetz im formellen Sinn vorgesehen sein muss. Um es anders zu formulieren: Die Gesichtserkennung zum Zwecke der Identifikation basiert, wie einführend erklärt, auf einem Abgleich von 1:n. Für die Bearbeitung von 1 und von n sowie den Abgleich selbst braucht es gesetzliche Grundlagen, für Letzteres in jedem Fall eine formell-gesetzliche und damit besonders demokratisch legitimierte.

2. Rechtmässigkeit de lege lata

Es gilt nun zu klären, ob sich der polizeiliche Einsatz von Gesichtserkennungssoftware in der Schweiz bereits auf eine gesetzliche Grundlage (auf ausreichender Normstufe und mit hinreichender Normdichte) oder alternativ auf das im Polizeirecht zur Verfügung stehende Surrogat, die polizeiliche Generalklausel, stützen kann.

Für die Anwendung der Generalklausel ist das Vorliegen der Gefährdung eines fundamentalen Rechtsguts (1.) und einer schwerwiegenden Gefahr (2.) verlangt. Ferner bedarf es der zeitlichen Dringlichkeit (3.), der Subsidiarität (4.) und Verhältnismässigkeit (5.) der Massnahme. Schliesslich muss die handelnde Behörde zuständig (6.) sein.[93] Ihr Heranziehen bedingt eine ernste und unmittelbar drohende Gefahr für die öffentliche Ordnung und fundamentale Rechtsgüter des Staates oder Privater.[94] Beim Einsatz von Gesichtserkennungssoftware handelt es sich um ein planbares Unterfangen. Während ein einzelner Einsatz theoretisch noch der Bewältigung eines echten und unvorhersehbaren Notfalls dienen könnte, qualifiziert die Implementierung von Videoüberwachungen oder anderweitigen Datensammlungsmethoden, die Beschaffung von Gesichtserkennungstechnologie und die Bereitstellung der entsprechenden Datenbanken keineswegs als echter und unvorhersehbarer Notfall. Dies gilt für alle Einsatzbereiche. Die Gesichtserkennung lässt sich somit nicht auf die polizeiliche Generalklausel stützen.[95]

Bei der Suche nach einer Rechtsgrundlage für die automatisierte Gesichtserkennung ist nach ihrem Einsatzbereich zu unterscheiden. Für die allgemeine Überwachung sind das kantonale Recht und insbesondere die kantonalen Polizeigesetze massgeblich. Das gilt auch für die konkrete Überwachung, wobei der Übergang von präventiv-polizeilichen Vorermittlungen zu strafprozessualen Ermittlungen in der Praxis fliessend sein kann. Für Letztere ist sodann die eidgenössische Strafprozessordnung heranzuziehen (Art. 15 Abs. 1 StPO[96]).

[84] Vgl. BGE 143 I 253 E. 4.4 ff. (259 f.); vgl. BSK-DSG-Jöhri/Studer, Art. 17 N 25; Müller (FN 38), 207 f.

[85] Vgl. zur Videoüberwachung im Allgemeinen Müller (FN 38), 209; BSK DSG-Jöhri/Studer, Art. 17 N 26; Tiefenthal, Polizeihoheit (FN 82), 367.

[86] Müller (FN 38), 130.

[87] Blonski (FN 23), 45 ff.

[88] Blonski (FN 23), 57 f.

[89] BBl 2020 7639 ff.

[90] So kann bei einer Analyse des Gesichtsbildes die betroffene Person meist einer ethnischen Gruppe zugeordnet werden, oder bei einer Retinaerkennung des Auges lässt sich durch eine Analyse der Gefässmuster auf bestimmte Krankheiten schliessen; dazu Blonski (FN 23), 58.

[91] Vgl. Hornung/Schindler (FN 39), 205 f.

[92] Vgl. z.B. für die Erstellung von Persönlichkeitsprofilen BGE 143 I 253 E. 3 ff. (257 ff.).

[93] Vgl. BGE 147 I 161 E. 5.1 (165 f.); BGE 137 II 431 E. 3.3.2 (445); BGE 136 IV 97 E. 6.3.2 (114 ff.); Tiefenthal, Polizeirecht (FN 38), § 6 N 3; BSK BV-Epiney, Art. 36 N 40 ff.

[94] BGE 137 II 431 E. 3.3.1 (444 f.); vgl. auch Tiefenthal, Polizeirecht (FN 38), § 6 N 1 ff.

[95] Vgl. für die Überwachung im öffentlichen Raum Tiefenthal, Polizeihoheit (FN 82), 368; Müller (FN 38), 203; BSK DSG-Jöhri/Studer, Art. 17 N 56.

[96] Schweizerische Strafprozessordnung vom 5. Oktober 2007 (Strafprozessordnung, StPO), SR 312.0.

2.1 Grundlagen im Strafprozessrecht

Dient die Gesichtserkennung der Klärung einer strafrechtlichen Verdachtslage und der Verfolgung von Straftaten, handelt es sich um polizeiliche Ermittlungstätigkeit im Rahmen von Strafverfahren.[97] Entscheidend für die Anwendbarkeit der StPO ist der Anfangsverdacht i.S.v. Art. 299 Abs. 2 StPO.[98] Die Aufgaben der Polizei im Ermittlungsverfahren umfassen neben der Sicherstellung von Spuren und Beweisen insbesondere die Ermittlung von tatverdächtigen Personen (Art. 306 Abs. 2 lit. b StPO). Dies kann unter Zuhilfenahme von Gesichtserkennungstechnologie geschehen.[99] Die Erkennung erfolgt durch einen nachträglichen Abgleich von Datenmaterial oder in Echtzeit. Beide Varianten stellen einen rechtfertigungsbedürftigen Grundrechtseingriff dar. Art. 306 StPO hält einen allgemeinen Ermittlungsauftrag fest. Dieser normiert zwar den Zweck polizeilicher Ermittlungen, verkörpert aber keine ausreichend spezifische Regelung konkreter Ermittlungsmassnahmen.[100] Als Grundlage für die Gesichtserkennung kommen ferner die Bestimmungen zu den Zwangsmassnahmen gemäss Art. 196 ff. StPO infrage, dient sie doch der Beweissicherung i.S.v. Art. 196 lit. a StPO. Oder es wird davon ausgegangen, dieses kriminalistische Instrument sei wie andere Datenbearbeitungen vom generellen Ermittlungsauftrag erfasst und könne sich schlicht auf Art. 95 ff. StPO stützen.

Der Katalog an strafprozessualen Zwangsmassnahmen hält mit relativ hohem Bestimmtheitsgrad fest, welche Massnahmen zu welchem Zweck ergriffen werden können. Der Katalog gilt als Numerus clausus.[101] Zwangsmassnahmen sind alle Verfahrenshandlungen der Strafbehörden, die in Grundrechte der Betroffenen eingreifen (Art. 196 StPO). So sieht Art. 210 Abs. 1 StPO betreffend die Fahndung vor, dass bei Fahndungen Personen zur Ermittlung ihres Aufenthaltsortes ausgeschrieben werden können. *E contrario* kann aus dieser Formulierung abgeleitet werden, dass zu Fahndungszwecken keine Echtzeit-Gesichtserkennungsanalyse durchgeführt werden darf, bei der z.B. alle in der Schweiz gerade im Einsatz stehenden Videoüberwachungssysteme «durchforstet» werden. Auch andere Instrumente wie die DNA-Analyse sind in Art. 255 ff. StPO explizit vorgesehen, auch – weniger eingriffsintensiv – die erkennungsdienstliche Erfassung von Körpermerkmalen in Art. 260 ff. StPO. Bei der erkennungsdienstlichen Erfassung oder der DNA-Analyse ist insbesondere der «erste Eingriff» in das Grundrecht geregelt. Es könnte in Bezug auf die Gesichtserkennung nun argumentiert werden, dass die erstmalige Erfassung des Bildmaterials via Videoüberwachung, erkennungsdienstlicher Massnahme oder auch mittels Beschlagnahme sowie Edition einer formell-gesetzlichen Grundlage bedarf, nicht jedoch deren weitergehende Analyse. Bei der Gesichtserkennung i.e.S. handelte es sich diesem Verständnis zufolge um ein herkömmliches Instrument der Kriminalanalyse, nicht viel anders als das Programm Excel oder andere Datenanalyseinstrumente. Die Gewinnung der Ausgangs- und Abgleichsdaten richtete sich demzufolge nach den Bestimmungen über die jeweiligen Zwangsmassnahmen oder z.B. auch denjenigen über die Überwachung mit technischen Überwachungsgeräten nach Art. 280 ff. StPO. Herangezogene Datenbanken fänden ihre Rechtsgrundlage sodann allenfalls im kantonalen Polizeirecht (siehe z.B. die POLIS-Verordnung des Kantons Zürich[102]). Handelt es sich um *open source information*, dürfte der Rückgriff auf die Datenbank weniger heikel sein. Auch dabei handelt es sich jedoch um eine staatliche Bearbeitung von Personendaten.[103] Aber sogar wenn die Gewinnung der Ausgangsdaten und diejenige der Abgleichsdaten in einem Gesetz vorgesehen sind – was je nach Gewinnungsart der Fall sein kann –, verbliebe dennoch die Frage nach dem Prozess des Datenabgleichs selbst, d.h. der eigentlichen automatisierten biometrischen Analyse der Gesichter. Wie ausgeführt, handelt es sich dabei um einen schweren Grundrechtseingriff. Dieser ist weder in der StPO noch in Polizeigesetzen normiert.

Im 8. Kapitel der StPO («Allgemeine Verfahrensregeln») widmen sich die Art. 95 ff. StPO der Datenbearbeitung und bilden die allgemeinen rechtlichen Grundlagen zur Bearbeitung von Personendaten in hängigen Strafverfahren.[104] Diese Bestimmungen stellen, wenn auch eher implizit, klar, dass die Strafbehörden zur Erfüllung ihrer Aufgaben im Strafverfahren Daten bearbeiten dürfen. Mit ihnen sollten die Grundsätze des Datenschutzrechts in die StPO übernommen werden.[105] Die Art. 95 ff. StPO stellen bloss allgemeine Grundsätze dar, die – gerade in Anbetracht der üblichen strafprozessrechtlichen Ansprüche – nur sehr wenig bestimmt sind. Als Rechtsgrundlage für die mit der Gesichtserkennung einhergehenden (schweren) Grundrechtseingriffe taugen sie nicht. Die automatisierte Gesichtserkennung unterscheidet sich qualitativ von der manuellen Sichtung. Die automatisierte Analyse biometrischer Daten stellt auch zu Beweiszwecken einen besonderen Grundrechtseingriff dar. Einen solchen Eingriff auf allgemeine Verfahrensregeln bzw. Generalklauseln zu stützen, würde den Anforderungen von Art. 36 Abs. 1 BV nicht gerecht.

[97] Vgl. Niklaus Oberholzer, Grundzüge des Strafprozessrechts, 4. Aufl., Bern 2020, N 88.

[98] BSK StPO II-Rhyner, Art. 306 N 6; Oberholzer (FN 97), N 91; vgl. auch Niklaus Schmid/Daniel Jositsch, Handbuch des schweizerischen Strafprozessrechts, 3. Aufl., Zürich/St. Gallen 2017, N 1217.

[99] Vgl. dazu das Beispiel bei Luchetta (FN 6), 39.

[100] Vgl. BSK StPO II-Rhyner, Art. 306 N 19 f.; vgl. auch Oberholzer (FN 97), N 1780.

[101] Anstatt vieler BSK StPO II-Weber, Art. 197 StPO N 4.

[102] Verordnung über das Polizei-Informationssystem POLIS vom 13. Juli 2005 (POLIS-Verordnung), LS 551.103. Im Übrigen besteht auch für den Bund im Bundesgesetz über die polizeilichen Informationssysteme des Bundes vom 13. Juni 2008 (BPI), SR 361, keine hinreichend bestimmte Gesetzesgrundlage für einen Datenabgleich.

[103] Siehe die Diskussion bei Anna Cartner/Sandra Schweingruber, Strafbehörden dürfen googlen, AJP 8/2021, 990 ff., 993 f. Gemäss den Autorinnen kann sich die Beschaffung von *open source information* auf Art. 95 StPO abstützen. Dies überzeugt aufgrund des tiefen Bestimmtheitsgrads dieser allgemeinen Regel für die Bearbeitung von besonders schützenswerten Personendaten nicht restlos.

[104] Vgl. BSK StPO I-Fiolka, Vor Art. 95 ff. N 2.

[105] SK-StPO-Brüschweiler/Grünig, Art. 95 N 1; BSK StPO I-Fiolka, Vor Art. 95 ff. N 1.

Ähnlich wie die erkennungsdienstliche Erfassung (oder sogar weitergehender) wäre die Erstellung von Templates und deren Abgleich durch die Polizei explizit als Zwangsmassnahme vorzusehen. Ansonsten könnten die Art. 95 ff. StPO auch schlicht für jeden strafprozessualen Eingriff in Art. 13 Abs. 2 BV «herhalten».

Für den strafprozessualen Bereich lässt sich also festhalten, dass die Beurteilung der Rechtmässigkeit einerseits davon abhängt, ob man unter der Gesichtserkennung eine selbstständige Zwangsmassnahme versteht, die gesetzlich eigens normiert werden müsste. Dies ist zu bejahen. Andererseits ist massgeblich, für wie weitreichend man die Art. 95 ff. StPO klassifiziert. Diese bestehenden Normen sind nicht als hinreichend bestimmt zu erachten, um den Grundrechtseingriff der Gesichtserkennung i.e.S. zu rechtfertigen. Zumeist dürfte es ferner an einer Grundlage für die Beschaffung der Abgleichsdaten fehlen, müsste doch auch diese strafprozessuale Massnahme (und Zwecksetzung) in einer Norm festgehalten sein.

2.2 Grundlagen im Polizeirecht

Für die Anwendungen der Gesichtserkennung, welche nicht auf einem Anfangsverdacht basieren, müssten – im Falle der Verbreitung derartiger Technologie bei den Schweizer Polizeikorps – kantonale Rechtsgrundlagen bestehen. Die Regelung des Einsatzes technischer Überwachungsgeräte (wie der Videoüberwachung) zu sicherheits- und präventivpolizeilichen Zwecken unterliegt der kantonalen Polizeihoheit.[106] Gestützt darauf hat die Mehrheit der Kantone die Videoüberwachung im kantonalen Polizeigesetz normiert.[107] So erlaubt es z.B. § 32b des Zürcher Polizeigesetzes (PolG ZH)[108] der Polizei, den öffentlich zugänglichen Raum in der Weise mit Audio- und Videogeräten zu überwachen, dass Personen identifiziert werden können, sofern am überwachten Ort Straftaten bereits begangen worden sind bzw. mit solchen zu rechnen ist. Vergleichbares gilt gemäss § 32c PolG ZH bei Grossveranstaltungen oder Kundgebungen. Damit bestehen im Kanton Zürich gesetzliche Grundlagen für den Einsatz von Videoüberwachung, welche eine Personenidentifikation zulässt. Diese umfassen in ihrer jetzigen Formulierung die Nutzung von Gesichtserkennungstechnologie nicht. Die Gesichtserkennung erfordert eine weitere Datenbearbeitung (Datenabgleich). Jede weitere Bearbeitung des Bildmaterials und damit auch eine biometrische Auswertung von Gesichtern, d.h. die Erstellung von Templates und deren Abgleich, wären hinreichend bestimmt (formell-)gesetzlich vorzusehen.[109]

Regelungen zur Videoüberwachung, zur Datenbearbeitung und zum Datenaustausch enthält auch das Polizeigesetz des Kantons Basel-Landschaft (PolG BL[110]). Gemäss § 45b Abs. 1 PolG BL kann die Polizei bei öffentlichen Veranstaltungen oder Kundgebungen allgemein und nicht allgemein öffentlich zugängliche Orte bei Vorliegen gewisser Bedingungen mit technischen Geräten offen überwachen. Bezüglich Datenbearbeitung hält § 45b Abs. 3 PolG BL fest, unter welchen Voraussetzungen die Aufzeichnungen bearbeitet werden dürfen. Das PolG BL enthält damit eine Rechtsgrundlage für die polizeiliche Überwachung des öffentlichen Raumes und die anschliessende (stark eingeschränkte) Bearbeitung der Aufzeichnungen. Eine Grundlage für einen automatisierten Abgleich der in den Aufzeichnungen erfassten Gesichtern mit anderen Daten ist jedoch nicht vorgesehen. Spezifisch normiert ist ein Datenabgleich jedoch in Art. § 45f PolG BL für die automatisierte Fahrzeugfahndung und Verkehrsüberwachung (AFV).[111] Die Norm erlaubt der Polizei die automatisierte Erfassung von Kontrollschildern sowie einen direkten Abgleich mit Fahndungsdatenbanken.

Anhand der Rechtsprechung zur AFV lassen sich wichtige Erkenntnisse für die rechtliche Würdigung des polizeilichen Einsatzes von Gesichtserkennungstechnologie gewinnen. Das Bundesgericht beurteilte 2019 die Rechtmässigkeit der AFV im Kanton Thurgau: Das Erheben und Aufbewahren der Aufzeichnungen durch die AFV stellt gemäss Bundesgericht eine erkennungsdienstliche Massnahme dar und fällt in den Schutzbereich von Art. 13 Abs. 2 BV. Da die AFV nicht nur die Erhebung und Aufbewahrung von erkennungsdienstlichen Daten, sondern auch eine Zusammenführung mit anderen Datensammlungen sowie einen automatisierten Abgleich umfasse, handle es sich bei ihr um einen schweren Grundrechtseingriff. Das System ermögliche die serielle und simultane Verarbeitung grosser und komplexer Datensätze innert Sekundenbruchteilen, was über die herkömmlichen verkehrstechnischen Informationsbeschaffungen und Fahndungssysteme hinausgehe. Zudem könne das System durch Kombination mit anderen Daten und durch ihre grosse Streuweite gar Grundlage für Persönlichkeits- oder Bewegungsprofile bilden. Es wäre folglich eine ausdrückliche und hinreichend bestimmte Regelung in einem Gesetz im formellen Sinne vorzusehen gewesen.[112] Eine solche lag im Kanton Thurgau nicht vor, da weder der Verwendungszweck der Datenerhebung klar umschrieben noch die Reichweite des Datenabgleichs eingegrenzt wurde. Darüber hinaus müsse eine Löschungspflicht für nicht weiter verwendete Daten vorgesehen werden, da sonst

[106] Tiefenthal, Polizeirecht (FN 38), § 21 N 1; vgl. z.B. BGE 140 I 353 E. 5.1. (359 f.).
[107] Siehe den Überblick in Tiefenthal, Polizeirecht (FN 38), § 21 N 16 ff.
[108] Polizeigesetz des Kantons Zürich vom 6. Februar 2007 (PolG), LS 550.1.
[109] Vgl. Müller (FN 38), 231.
[110] Polizeigesetz des Kantons Basel-Landschaft vom 28. November 1996 (PolG), SGS 700.
[111] Auch das Aargauer Gesetz über die Gewährleistung der öffentlichen Sicherheit vom 6. Dezember 2005 (Polizeigesetz, PolG), SAR 531.200, sieht in Art. 36b eine derartige Regelung der AFV vor.
[112] Siehe auch Elias Krummenacher/Nicole Ebneter, Bundesgericht, Strafrechtliche Abteilung, Urteil 6B_908/2018 vom 7. Oktober 2019 (zur Publikation vorgesehen), A. gegen Generalstaatsanwaltschaft des Kantons Thurgau, Verwertbarkeit von Beweisen (mehrfaches Fahren ohne Berechtigung), AJP 2/2020, 221 ff.

eine Sammlung von erkennungsdienstlichen Daten auf Vorrat erlaubt wäre.[113]

Das Bundesgericht stellt somit hohe Anforderungen an die gesetzlichen Grundlagen von automatisierten Erkennungssystemen. Insbesondere muss ein allfälliger Datenabgleich auf einer hinreichend bestimmten gesetzlichen Grundlage gründen. Übertragen auf die (eingriffsintensivere) automatisierte Gesichtserkennung bedeutet dies, dass der Datenabgleich (Gesichtserkennung i.e.S.) in einer gesetzlichen Grundlage vorgesehen werden muss. Zusätzlich wäre jeweils auch eine gesetzliche Grundlage für die Datengewinnung der Ausgangs- und Abgleichsdaten zu schaffen. Sollten Polizeikorps die Gesichtserkennungstechnologie zum Zwecke der allgemeinen oder konkreten Überwachung einsetzen wollen, wären hinreichend bestimmte gesetzliche Grundlagen für alle Elemente des Gesichtserkennungsprozesses vorzusehen. Solche finden sich heute in keinem Kanton. Somit lässt sich resümieren, dass *de lege lata* weder im Polizei- noch im Strafprozessrecht ausreichende Rechtsgrundlagen für den polizeilichen Einsatz automatisierter Gesichtserkennung bestehen. Der Einsatz ist aktuell nicht rechtmässig.[114]

3. Regulierung de lege ferenda

Der Einsatz von Gesichtserkennungssoftware durch Schweizer Polizeikorps (wenn auch teilweise nur im Rahmen von Tests) ist aktuell rechtlich nicht vorgesehen. Es ist deshalb zu diskutieren, ob und wie die automatisierte Gesichtserkennung zu regulieren ist. Jedenfalls sind eine solche Diskussion sowie eine allfällige demokratische Legitimierung (bzw. Nicht-Legitimierung) nötig. Eine «schleichende» Etablierung der Technologie, wie sie sich gerade abzeichnet, ist hingegen zu verhindern. Es bestehen verschiedene Möglichkeiten der Regulierung. Diese reichen von einem expliziten Verbot über eine punktuelle Regelung in StPO und kantonalen Gesetzen bis hin zu einer spezialgesetzlichen Regelung des Einsatzes, wobei stets die verschiedenen Varianten der Gesichtserkennung zu differenzieren sind.

3.1 Absolutes Verbot oder Abstufung

Vorab ist anzumerken, dass es natürlich nicht ausgeschlossen ist, sich der Regulierung der Gesichtserkennungstechnologie (noch) nicht anzunehmen. Wird trotz anhaltenden Diskurses keine Rechtsgrundlage für den Einsatz von Gesichtserkennungssystemen geschaffen, wäre dies als qualifiziertes Schweigen des Gesetzgebers zu interpretieren.[115] Da sich weder der eidgenössische noch die kantonalen Gesetzgeber aktuell mit der Materie intensiver beschäftigt haben, kann jedoch im Moment nicht von einer solchen impliziten Verhinderung des Einsatzes ausgegangen werden.

In Anbetracht der ausführlich beschriebenen Grundrechtseingriffe, die mit der automatisierten Gesichtserkennung einhergehen, ist es eine naheliegende Lösung, diese zu Überwachungs- und Strafverfolgungszwecken schlicht zu verbieten. Es wäre angesichts der mannigfaltigen Anwendungsmöglichkeiten dieser Technologie allerdings ebenso denkbar, eine abgestufte bzw. differenzierte Regelung zu erlassen. So könnte der punktuelle Einsatz, z.B. der Datenabgleich zu Beweiszwecken im Strafverfahren, zwar an Bedingungen geknüpft, aber dennoch ermöglicht werden. Eine solche abgestufte Regelung sieht der EU-KI-Verordnungsvorschlag vor.[116] Im Entwurf wird risikoorientiert eine Differenzierung vorgenommen: Bestimmte, mit einem als inakzeptabel erachteten Risiko verbundene Praktiken der KI werden verboten. Konkret untersagt Art. 5 Abs. 1 lit. d EU-KI-Verordnungsvorschlag den Einsatz von biometrischen Echtzeit-Fernidentifizierungssystemen in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken. Eine Ausnahme davon wird gemacht i) für die gezielte Suche nach bestimmten potenziellen Opfern von Straftaten oder nach vermissten Kindern, ii) für das Abwenden einer konkreten, erheblichen und unmittelbaren Gefahr für das Leben oder die körperliche Unversehrtheit natürlicher Personen oder eines Terroranschlags und iii) für das Erkennen, Aufspüren, Identifizieren oder Verfolgen eines Täters oder Verdächtigen gewisser schwerer Straftaten. Für einen Katalog an Szenarien ist die automatisierte Gesichtserkennung also durchaus erlaubt. Allerdings sind auch dann gewisse Vorkehrungen zu treffen und es ist vorgängig die Genehmigung einer unabhängigen Verwaltungs- oder Justizbehörde einzuholen (Art. 5 Abs. 3). Neben der «biometrischen Echtzeit-Fernidentifizierung» ist auch die «nachträgliche biometrische Fernidentifizierung natürlicher Personen» als «Hochrisiko-KI-System» klassifiziert (Anhang III Ziff. 1 lit. a). Bei derartigen Systemen sind gewisse Anforderungen einzuhalten, so ist z.B. ein Risikomanagement, eine Daten-Governance und eine menschliche Aufsicht sicherzustellen (Art. 8 ff.).

Ein solcher Weg wäre auch für die Schweiz gangbar, wobei zur Abstufung der Regelung die vorne in Kap. III.3 dargestellten Varianten der Gesichtserkennung dienen können. So könnte beispielsweise die Echtzeit-Gesichtserkennung zu allgemeinen oder konkreten Überwachungszwecken verboten, im Bereich der Strafverfolgung jedoch unter gewissen Voraussetzungen erlaubt werden. Auch hier wären allerdings Standards zu etablieren, welchen die Technologie und ihr Betrieb zu genügen haben. Möglich – aber wahrscheinlich eher untypisch für die Schweiz – wäre ein Verbot bzw. ein «Teilverbot» nach dem Vorbild der EU in einem Gesetz über die KI.[117] Eine solche Normierung, die insbesondere auch die präventiv-polizeilichen Einsätze der Gesichtserkennung umfassen müsste, würde jedoch an

[113] BGE 146 I 11 E. 3.1 ff. (13 ff.).

[114] Wird von solchen technischen Hilfsmitteln im Strafprozess dennoch Gebrauch gemacht, führt dies grundsätzlich zur Unverwertbarkeit der damit erlangten Beweismittel; vgl. eingehend dazu BGE 146 I 11, E. 4.2 (19).

[115] Zur Regelung durch qualifiziertes Schweigen des Gesetzgebers siehe allgemein z.B. BGE 145 IV 252 E. 1.6.1 ff. (256 ff.).

[116] Vorne FN 10.

[117] Vgl. Braun Binder et al. (FN 3), N 55.

der fehlenden Bundeskompetenz zur Legiferierung im sicherheitspolizeilichen Bereich scheitern. Die Etablierung einer «dezentralen» Regelung in kantonalen Polizeigesetzen, der StPO und/oder einem Spezialgesetz erscheint deshalb vielversprechender.

3.2 Regelung in Polizeigesetzen, der StPO oder einem Spezialgesetz

Will der Gesetzgeber den präventiv-polizeilichen Einsatz von Gesichtserkennungstechnologie ermöglichen, wären dafür geeignete Rechtsgrundlagen im kantonalen Polizeirecht zu schaffen. Entsprechende Normen hätten zunächst den Zweck des Einsatzes automatisierter Gesichtserkennung einzugrenzen. Des Weiteren wären neben der Erhebung des Datenmaterials (i.d.R. mittels Videoüberwachung) der Modus des Datenabgleichs (Echtzeit- oder nachträgliche Analyse) sowie der Datenabgleich selbst (Gesichtserkennung i.e.S.) gesetzlich zu normieren. Eine spätere Speicherung und Wiederverwendung von Gesichtstemplates wäre selbstverständlich ebenfalls explizit formell-gesetzlich festzuhalten.

Ein strafprozessualer Einsatz bedürfte entsprechender Bestimmungen in der StPO. Die Gesichtserkennung müsste als Zwangsmassnahme eingeführt werden. Auch hier müssten der Zweck, die Gewinnung der Ausgangs- und Abgleichsdaten sowie die Gesichtserkennung selbst normiert werden. Der Rechtssetzungsprozess – insbesondere derjenige auf Bundesebene – erlaubte eine breitere Diskussion über die Legitimität des Einsatzes dieser Technologie. Diesem zunehmend dringlichen Diskurs förderlich wäre die Option, die Gesichtserkennungstechnologie mit dem Erlass eines Spezialgesetzes zu regulieren. Der Vorteil einer spezialgesetzlichen Regelung besteht in der Möglichkeit, die Anwendung der Technologie in hoher Dichte zu normieren. So könnten, den Risiken der verschiedenen Einsatzbereiche entsprechend, differenzierte Regelungen vorgenommen werden. Die Regulierung einer bestimmten Technik stellt für die Strafrechtspflege und Polizeiarbeit indessen kein Neuland dar. So wurde beispielsweise die Verwendung von DNA-Profilen und -analysen im DNA-Profil-Gesetz[118] bundesrechtlich geregelt. Mit der Einführung der schweizerischen StPO wurden die Gesetzesgrundlagen zu den DNA-Analysen jedoch in die StPO überführt (Art. 255 ff. StPO). Für den Bereich der Strafverfolgung wäre eine Regelung in der StPO deshalb ebenfalls naheliegender. Aufgrund der Kompetenzverteilung zwischen Bund und Kantonen könnte zudem ohnehin keine umfassende spezialgesetzliche Regulierung der Technologie auf Bundesebene erfolgen.

V. Fazit

Neue «smarte» Technologien erobern die Polizeiarbeit und Strafrechtspflege, darunter auch verheissungsvolle Gesichtserkennungssoftware. Die automatisierte Gesichtserkennung verspricht mehr Effektivität und Effizienz, birgt jedoch – wie jeder Einsatz von KI im Überwachungs- und Strafverfolgungsbereich – Risiken. Dieser Beitrag konnte aufzeigen, dass für ihren Einsatz weder im Strafprozessrecht noch im kantonalen Polizeirecht ausreichende Rechtsgrundlagen vorhanden sind. Der Einsatz von Gesichtserkennungstechnologie ist folglich unrechtmässig. Dennoch nutzen erste Kantone derartige Anwendungen. Eine solche übereilte Implementierung, in deren Vorfeld keine fundierte Auseinandersetzung mit den rechtlichen Grundlagen und der Funktionsweise stattfindet, ist zu kritisieren. «Smart» geht anders.

Die vertiefte Auseinandersetzung mit dem polizeilichen Einsatz von Gesichtserkennungstechnologie hat gezeigt, dass sich der damit einhergehende Prozess in drei Phasen gliedert: die Gewinnung der Ausgangsdaten, die Gewinnung der Abgleichsdaten und die Gesichtsanalyse selbst, d.h. die biometrische Verarbeitung und der biometrische Abgleich. Soll der Einsatz dieser Technologie in einem der möglichen Einsatzbereiche (allgemeine Überwachung, konkrete Überwachung oder Strafverfolgung) rechtlich erlaubt werden, wären alle Elemente zu normieren und die damit einhergehenden Grundrechtseingriffe zugleich zu begrenzen. Diese Grundrechtseingriffe wiegen nämlich potenziell sehr schwer.

Am schwersten wiegen die Eingriffe in die persönliche Freiheit bei der allgemeinen Überwachung. Dieser Eingriff in die Grundrechte zahlreicher Personen, welche dazu keinen Anlass geboten haben, ist kaum zu rechtfertigen. Dies gilt insbesondere für die Echtzeit-Überwachung. Hier ist dem EU-Vorschlag zu folgen, welcher diese Art der Überwachung grundsätzlich für unzulässig erklärt. Ähnliches kann auch für die konkrete Überwachung gelten. Die Vornahme der biometrischen Gesichtsanalyse zu präventiven Zwecken, z.B. in Fussballstadien wie in Wales, ist – sowohl in Anbetracht des aktuellen Entwicklungsstands der Technologie als auch aus generellen gesellschaftspolitischen Gründen – ebenfalls nicht oder nur mit sehr hohen Hürden zu erlauben. Für die Aufklärung von schweren Straftaten könnte die Nutzung der zweifellos auch Potenzial bergenden Gesichtserkennungstechnologie hingegen in Betracht gezogen werden. Auch hier ist allerdings Zurückhaltung geboten. Insbesondere müsste der Einsatz der automatisierten Gesichtserkennung in der Strafverfolgung an klare Bedingungen geknüpft und eine gerichtliche Genehmigung verlangt werden.

Die Nutzung von Gesichtserkennungssystemen durch die Polizei ist Realität und dürfte rasant zunehmen. Der Gesetzgeber hat Nachholbedarf, ebenso die öffentliche Debatte. Gesichtserkennungstechnologie kann Teil einer Smart Criminal Justice werden. Dafür braucht es jedoch einen definierten Rechtsrahmen – und eben etwas «Smartness».

[118] Bundesgesetz über die Verwendung von DNA-Profilen im Strafverfahren und zur Identifizierung von unbekannten oder vermissten Personen vom 20. Juni 2003 (DNA-Profil-Gesetz), SR 363.