

Die Unrechtmässigkeit des Einsatzes automatisierter Gesichtserkennung im Strafverfahren – ein weiterer Beitrag zu einer anhaltenden Debatte

MONIKA SIMMLER*/GIULIA CANOVA**

Schlagwörter: Automatisierte Gesichtserkennung, Face Recognition, Biometrische Analysen, Digitale Ermittlungen, Strafprozessrecht

A. Bisherige Debatte

Seit der Veröffentlichung unserer ersten Publikation¹ zur (Un-)Rechtmässigkeit der automatisierten Gesichtserkennung in Polizei- und Strafprozessrecht im Winter 2021 hat sich die Debatte rund um den Einsatz von Gesichtserkennungstechnologie um einiges intensiviert. Nicht nur erschien auf unseren Beitrag hin eine uns widersprechende Replik, die den Standpunkt vertrat, der Einsatz automatisierter Gesichtserkennung erfolge in Strafverfahren rechtmässig,² sondern es kam in den zwei Jahren auch zu einer Vielzahl an Medienberichten.³ Dieser wissenschaftliche und öffentliche Diskurs ist wichtig. Es handelt sich bei der automatisierten Gesichtserkennung, d.h. dem Einsatz automatisierter biometrischer (Massen-)Analyseverfahren zur Identifikation natürlicher Personen um eine neue Überwachungs- und Ermittlungsmethode, die nicht ohne Grund Fragen aufwirft und kritisch reflektiert wird.

* Prof. Dr., Assistenzprofessorin für Strafrecht, Strafprozessrecht und Kriminologie an der Universität St. Gallen.

** M.A. HSG in Law and Economics, Wissenschaftliche Mitarbeiterin an der Universität St. Gallen.

1 MONIKA SIMMLER/GIULIA CANOVA, Gesichtserkennungstechnologie: die «smarte» Polizeiarbeit auf dem rechtlichen Prüfstand, *Sicherheit & Recht* 2021, S. 105–117.

2 STEFAN KÜHNE, Automatisierte Bearbeitung von Personendaten im Polizei- und Strafprozessrecht, *Sicherheit & Recht* 2022, S. 13–24.

3 Siehe z.B. SRF Rundschau vom 26.01.2022, «Totale Überwachung: Streit um digitale Verbrechenjagd»; NZZ vom 02.07.2022, «Polizeikorps nutzen automatisierte Gesichtserkennung für die Fahndung»; SRF Schweiz aktuell vom 15.09.2022, «Schweizer Städte wollen keine automatische Gesichtserkennung»; Schweizer Monat Mai 2021, «Darf das die Polizei?».

Zum ersten Mal soll Künstliche Intelligenz (KI) in Strafverfahren zur Ermittlung eingesetzt werden. Es entlädt sich an dieser Debatte folglich auch das Spannungsfeld zwischen den Chancen technologischen Fortschritts für die Aufklärung von Straftaten und den Sorgen hinsichtlich ihres Missbrauchspotenzials. Darüber hinaus wird der KI aktuell nicht zugetraut, diskriminierungsfrei sowie ausreichend treffsicher zu sein.⁴ Der Umgang mit sog. Biases, d.h. potenziell diskriminierenden Verzerrungen, die KI-Verfahren inhärent sein können, wird mit der Gesichtserkennungstechnologie erstmals anhand eines konkreten Beispiels im Strafverfahren diskutiert.⁵ Mit Blick auf das Strafprozessrecht stellen sich ferner Fragen, die über die diskutierte Anwendung hinaus Bedeutung haben. Die Auseinandersetzung mit der biometrischen Datenanalyse sowie dem Datenabgleich zum Zwecke der Gesichtserkennung zeigt schnell, dass der traditionelle und statische Fokus geltender Rechtsgrundlagen auf die Datenbeschaffung es nicht vermag, diese Grundrechtseingriffe in Form von neuartigen Datenanalysen geeignet abzubilden.

Wir haben in unserer ersten Publikation zur Rechtmässigkeit der automatisierten Gesichtserkennung im Strafverfahren Stellung bezogen und diese verneint. In Anbetracht der strengen bundesgerichtlichen Rechtsprechung zur automatisierten Fahrzeugfahndung und Verkehrsüberwachung (AFV)⁶ und in Übereinstimmung mit der Datenschutzgesetzgebung gehen wir davon aus, dass jede Bearbeitung von besonders schützenswerten Personendaten einer formell-gesetzlichen Grundlage bedarf. Das gilt auch für die automatisierte Gesichtserkennung. Diese ist weder in der Strafprozessordnung (StPO) noch andernorts in der erforderlichen Bestimmtheit geregelt. Die Rechtmässigkeit ihres Einsatzes ist deshalb zu verneinen.

Diesen Standpunkt wollen wir in diesem Beitrag erneut vertreten und vertieft begründen. In Anbetracht der Debatte wurde deutlich, wie wichtig es ist, stets klarzustellen, auf welche Art und welchen Einsatzbereich automatisierter Gesichtserkennung Bezug genommen wird. Prävention und Repression werden oft vermischt oder es wird zu wenig präzisiert, was genau mit «Gesichtserkennung» gemeint ist. Dieser Beitrag soll deshalb auch zu einer weiteren Differenzierung der Debatte beitragen, insbesondere mit Blick auf eine mögliche Rechtsfortentwicklung.

In diesem Sinne werden wir nachfolgend zunächst erläutern, auf welchem Verfahren die automatisierte Gesichtserkennung beruht und welche Arten und Einsatzbereiche zu unterscheiden sind (Kap. B). In der Folge werden wir darlegen, weshalb Einsätze automatisierter Gesichtserkennung einen (schweren)

4 Vgl. MURAT KARABOGA et al., Automatisierte Erkennung von Stimme, Sprache und Gesicht, Zürich 2022, S. 121 ff.

5 Siehe z.B. NADJA BRAUN BINDER/ELIANE KUNZ/LILIANE OBRECHT, Maschinelle Gesichtserkennung im öffentlichen Raum, *sui-generis* 2022, N 31 f.; vgl. KARABOGA et al. (Fn. 4), S. 122.

6 Grundlegend BGE 146 I 11; kürzlich bestätigt in BGer 1C_39/2021 v. 29.11.2022.

Grundrechtseingriff darstellen (Kap. C), sowie systematisch alle Rechtsgrundlagen abhandeln, die in der Debatte zur Rechtfertigung der Gesichtserkennung vorgebracht wurden (Kap. D und E). Eines der Hauptargumente sei vorweggenommen: Wenn in einer Debatte so viele verschiedene mögliche Rechtsgrundlagen für eine Ermittlungsmethode vorgebracht werden, ist dies als sehr starkes Indiz zu werten, dass die Bestimmtheit dieser Rechtsgrundlagen ungenügend ist. Wie die Regulierung in Zukunft angegangen werden könnte, wollen wir deshalb im Anschluss diskutieren, wobei ein besonderes Augenmerk auf die KI-Verordnung der EU gelegt wird (Kap. F).

B. Automatisierte Gesichtserkennung

I. Gesichtserkennung als Datenabgleich

Gesichtserkennung bedeutet schlicht die Zuordnung eines Gesichts zu einer bestimmten Person.⁷ Dies kann manuell durch die Sichtung von Gesichtsbildern oder technologiegestützt unter Beizug von Gesichtserkennungstechnologie erfolgen. Von automatisierter Gesichtserkennung ist die Rede, wenn digitale Bilder, die Gesichter natürlicher Personen enthalten, automatisch verarbeitet werden, um die Personen zu identifizieren, kategorisieren oder eine Identifikation zu verifizieren.⁸ Inputdaten in Form von Bild- oder Videomaterial werden verarbeitet, um daraus Daten mit einem neuen Informationsgehalt bspw. zu Identität, Emotionen oder demographischen Attributen einer Person zu generieren.⁹

Die Gesichtsverifikation basiert auf einem 1 : 1-Abgleich, bei dem ein erfasstes Gesicht mit einer Vorlage eines Gesichts abgeglichen wird.¹⁰ Die Gesichtsidentifikation hingegen operiert basierend auf einem 1 : n- oder n : 1-Abgleich, bei dem ein bestimmtes Gesicht auf der einen und eine Vielzahl von Gesichtern auf der anderen Seite miteinander abgeglichen werden.¹¹

Im Strafverfolgungskontext besteht das Anwendungspotenzial automatisierter Gesichtserkennung hauptsächlich darin, Bild- oder Videomaterial automatisch zu analysieren, um darin enthaltene Gesichter natürlicher Personen zu identifizieren, zumeist von Beschuldigten oder anderweitig an der Tat Beteiligten.¹² Im Zentrum

7 AMELIE P. HELDT, Gesichtserkennung: Schlüssel oder Spitzel?, *Multimedia und Recht* 2018, S. 285–289, S. 286.

8 BRAUN BINDER/KUNZ/OBRECHT (Fn. 5), N 12.

9 Vgl. ISABELLE HUPONT et al., The landscape of facial processing applications in the context of the European AI Act and the development of trustworthy systems, *Science Reports* 2022, S. 1–14, S. 1.

10 STAN Z. LI/ANIL K. JAIN, *Handbook of Face Recognition*, 2. Aufl., London 2011, S. 2.

11 Vgl. LI/JAIN (Fn. 10), S. 2 f.; DOMINIKA BLONSKI, *Biometrische Daten als Gegenstand des informationellen Selbstbestimmungsrechts*, Diss. Bern 2015, S. 12 f.

12 Vgl. SIMMLER/CANOVA (Fn. 1), S. 107; GERRIT HORNING/STEPHAN SCHINDLER, Das biometrische Auge der Polizei, *ZD aktuell* 2017, S. 203–209, S. 206 f.

stehen dürfte die Gesichtsidentifikation basierend auf einem 1 : n oder n : 1-Abgleich. Im Strafverfahren ist zwar auch die Verifikation im Sinne eines 1 : 1-Abgleichs einzelner Bilder mittels technischer Hilfsmittel von Bedeutung. Solche Anwendungen erfolgen jedoch nicht basierend auf automatisierten Datenbearbeitungen grosser Datenmengen, sondern eher im Sinne einzelner manueller – wenn auch technikgestützter – Vergleiche, die zumeist durch forensische Institute vorgenommen werden. Im Fokus dieser Abhandlung stehen automatisierte 1 : n- oder n : 1-Abgleiche, deren Rechtmässigkeit umstritten ist, und die zwangsläufig nicht nur einzelne Personen, sondern eine unbestimmte Zahl n Personen betreffen. So wird bei einem 1 : n-Abgleich überprüft, ob eine unbekannte Person X (z.B. ein Beschuldigter) in Bild- oder Videomaterial mit n Personen (z.B. einem Tankstellenvideo) wiederzuerkennen ist. Bei einem n : 1-Abgleich hingegen wird das Gesichtsbild einer unbekannten Person X (z.B. Person in einem Tankstellenvideo) automatisiert mit einer Datenbank von n-Gesichtern bereits identifizierter Personen (z.B. einer erkennungsdienstlichen Datenbank [ED-Datenbank]) abgeglichen.¹³ Ebenfalls denkbar ist ein n:n-Abgleich, mit dem bspw. abgeglichen wird, welche Gesichter sowohl im Bild- und Videomaterial als auch in Datenbanken erscheinen.

Die für den Abgleich verwendete Datengrundlage kann variieren. Es können digitale Gesichtsbilder mit ED-Datenbanken oder polizeilichem Überwachungsmaterial abgeglichen werden. Denkbar ist ferner ein Abgleich mit externen, von den Strafbehörden durch Zwangsmassnahmen (i.d.R. durch Beschlagnahme, ggf. auch via Rechtshilfe oder Aktenbeizug) beschafften Daten. Die Datengrundlage für den Abgleich kann auch aus öffentlich zugänglichen Daten bestehen, so z.B. durch Beizug der Software «Clearview AI», welche u.a. auf öffentlich zugängliche Daten aus sozialen Medien zurückgreift.¹⁴ Für die Invasivität der Massnahme spielt die Herkunft der Daten sowie die konkrete Funktionsweise des Systems eine Rolle. So greift Clearview AI z.B. auf Daten zu, deren Herkunft nicht immer klar ist. Andere Systeme hingegen sind insoweit «geschlossen», als dass sie nicht noch auf polizeiexterne Daten zurückgreifen.¹⁵

II. Gesichtserkennung als biometrisches Erkennungsverfahren

Die automatisierte Gesichtserkennung¹⁶ ist den klassischen biometrischen Erkennungsverfahren zuzuordnen, welche zur Identifikation oder Verifikation von

13 Dies entspricht den von KÜHNE (Fn. 2), S. 14 f., beschriebenen Szenarien des Abgleichs.

14 Gemäss Medienberichten wurde die Software von Clearview von Mitarbeitenden der Stadtpolizei Zürich und der Kantonspolizei St. Gallen getestet, Tagesanzeiger vom 06.09.2021, «Schweizer Polizisten testeten verbotene Gesichtserkennungs-App».

15 So z.B. auch die von der Kantonspolizei St. Gallen verwendete Software «Analyze DI Pro» von Griffeye, welche nur polizeiinternes Material verwendet, KARABOGA et al. (Fn. 4), S. 115.

16 Anstatt von Gesichtserkennung kann auch von einem «Gesichtsbildabgleich» gesprochen werden. Gesichtserkennungstechnologie dient dazu, die Gemeinsamkeiten von Bildern abzuglei-

natürlichen Personen an deren biometrische Merkmale anknüpfen.¹⁷ Sofern es sich nicht bloss um einen 1:1-Abgleich handelt, lokalisiert die Gesichtserkennungssoftware im Datenmaterial Gesichter, die in der Folge genauer biometrisch analysiert werden sollen. Bei dieser (insbesondere bei grossen Datenmengen) zumeist notwendigen vorgelagerten «Face Detection» wird festgestellt, bei welchen visuellen Objekten im Datenmaterial es sich überhaupt um menschliche Gesichter handeln könnte. Dafür kommt i.d.R. schlichte Objekterkennungstechnologie zum Einsatz.¹⁸ Im Anschluss an die Lokalisation eines Gesichts werden dann im ersten Schritt der Gesichtserkennung die Gesichtszüge als biometrische Merkmale einer Person maschinell erfasst. Dazu werden die Abstände zwischen definierten Punkten des Gesichts gemessen.¹⁹ Aus diesen Messdaten wird dann geometrisch eine biometrische Schablone des Gesichts generiert, die als «Template» in Form eines Datensatzes abgespeichert wird. Auf diese Weise werden die Gesichtszüge maschinenlesbar und können mit Schablonen anderer Gesichtsbilder maschinell verglichen werden.²⁰ In einem zweiten Schritt erfolgt die eigentliche Gesichtserkennung, und zwar durch einen Abgleich der Templates.²¹ Dabei wird das Template des Gesichts einer zu identifizierenden Person mit den anderen abgespeicherten bzw. erfassten Templates verglichen. Die geometrische Ähnlichkeit der Templates wird mathematisch berechnet. Ergibt der mathematische Abgleichsvorgang eine geometrische Ähnlichkeit im Bereich einer gewissen Toleranzschwelle, gelten die Gesichter als identisch.²²

III. Gesichtserkennung als Ermittlungsmassnahme

Die automatisierte Gesichtserkennung in der Polizeiarbeit kennt verschiedene Einsatzbereiche.²³ In der öffentlichen Debatte und in Medienbeiträgen wurden diese teilweise ungenügend differenziert,²⁴ was eine adäquate rechtliche Würdi-

chen, über die Fähigkeit eines eigentlichen «Erkennens» als subjektiver menschlicher Prozess verfügt sie hingegen nicht. In der vorliegenden Abhandlung wird – im Einklang mit der internationalen Literatur – trotzdem von Gesichtserkennung («Face Recognition») gesprochen.

17 BLONSKI (Fn. 11), S. 6; ASTRID ALBRECHT, Biometrische Verfahren im Spannungsfeld von Authentizität im elektronischen Rechtsverkehr und Persönlichkeitsschutz, Diss. Frankfurt, Baden-Baden 2003, S. 31.

18 Dieser erste Schritt des Gesichtserkennungsverfahrens wird auch als «Face Detection» bezeichnet, siehe dazu LI/JAIN (Fn. 10), S. 4; AHMAD TOLBA/ALI EL-BAZ/AHMED A. EL-HARBY, Face Recognition: A Literature Review, International Journal of Signal Processing, S. 88–103, S. 89.

19 RAMONA KEIST, Gesichtserkennung im zivilrechtlichen Persönlichkeitsschutz, Jusletter vom 20. 05. 2019, N 10.

20 NINA ELISABETH HERBERT, Digitale Bildnisse: Objektbezogene Interessengeflechte zwischen Urhebern, Abgebildeten und Nutzern in der digital-vernetzten Kommunikation, Diss. Berlin 2016, Tübingen 2017, S. 284 f.

21 BLONSKI (Fn. 11), S. 25; KEIST (Fn. 19), N 11.

22 HERBERT (Fn. 20), S. 285; BLONSKI (Fn. 11), S. 13; mit Blick auf den konkreten Anwendungsfall der Kantonspolizei St. Gallen auch KÜHNE (Fn. 2), S. 15.

23 Dazu bereits SIMMLER/CANOVA (Fn. 1), S. 108 ff.

24 So z.B. im Beitrag SRF Rundschau (Fn. 3).

gung verunmöglicht. Erstens kann die Technologie zur allgemeinen Überwachung öffentlich zugänglicher Räume eingesetzt werden. Dafür wird i.d.R. Videoüberwachungsinfrastruktur mit Gesichtserkennungstechnologie ergänzt, um sämtliche Personen, die einen überwachten Bereich passieren, zu identifizieren.²⁵ Es handelt sich hierbei um anlasslose Überwachungsmassnahmen,²⁶ die weder an das Vorliegen eines Tatverdachts noch an spezifische Vorkommnisse anknüpfen. Sie sind gänzlich dem präventiv-polizeilichen Einsatzbereich zuzurechnen.²⁷ Zweitens kann Gesichtserkennungstechnologie als konkrete Überwachungsmassnahme zur Gefahrenabwehr und Vorermittlung eingesetzt werden, so z.B. bei einer Demonstration, bei der an der Versammlung teilnehmende Personen beobachtet und so gleich identifiziert werden können. Im Rahmen solcher konkreter Überwachungsmassnahmen erfolgt die Nutzung anlassbezogen und ist auf Störungen oder störende Personen gerichtet.²⁸ Auch diese Variante ist dem Polizeirecht zuzuordnen. Vorliegend interessiert allerdings der dritte Einsatzbereich im Rahmen der Aufklärung von Straftaten. Erfolgt die automatisierte Gesichtserkennung repressiv, d.h. als Ermittlungsmassnahme im Nachgang von Straftaten, liegt ein strafprozessualer Einsatz vor, der in den Anwendungsbereich der StPO fällt.

Für die rechtliche Beurteilung der Gesichtserkennung ist weiter wichtig, ob die eingesetzten Systeme den Abgleich der Gesichtsdaten in Echtzeit oder nachträglich vornehmen.²⁹ In der Schweiz wird Echtzeit-Gesichtserkennung bis anhin polizeilich nur im Rahmen von automatisierten Passkontrollen an Flughäfen verwendet.³⁰ Bei der nachträglichen Gesichtserkennung werden Bild- oder Videoaufnahmen erst nach einem Ereignis mit Referenzdaten abgeglichen.³¹ Die meisten im Strafverfolgungskontext eingesetzten Systeme operieren auf nachträglicher Basis, so auch die von den kantonalen Polizeikörpers eingesetzten Systeme.³²

Wenn wir die Rechtmässigkeit der automatisierten Gesichtserkennung im Strafverfahren beurteilen, dann beziehen wir uns stets auf einen nachträglichen Einsatz als Ermittlungsmassnahme. Dass keine polizeirechtlichen Grundlagen in den Kantonen vorhanden sind, welche einen präventiven Einsatz automatisierter Gesichtserkennung legitimieren würden, ist unbestritten.³³

25 MARIO MARTINI, Gesichtserkennung im Spannungsfeld zwischen Sicherheit und Freiheit, *Neue Zeitschrift für Verwaltungsrecht – Extra* 2022, S. 1–16, S. 8.

26 MARTINI (Fn. 25), S. 8.

27 So bereits SIMMLER/CANOVA (Fn. 1), S. 108 f.; zum polizeirechtlichen Einsatz ebenfalls KÜHNE (Fn. 2), S. 17.

28 SIMMLER/CANOVA (Fn. 1), S. 109 f.

29 Vgl. BRAUN BINDER/KUNZ/OBRECHT (Fn. 5), N 10 ff., so auch bereits SIMMLER/CANOVA (Fn. 1), S. 111.

30 BRAUN BINDER/KUNZ/OBRECHT (Fn. 5), N 10.

31 Vgl. MARTINI (Fn. 25), S. 4.

32 Vgl. KARABOGA et al. (Fn. 4), S. 123; KÜHNE (Fn. 2), S. 14.

33 KÜHNE (Fn. 2), S. 19; SIMMLER/CANOVA (Fn. 1), S. 116; BRAUN BINDER/OBRECHT/KUNZ (Fn. 5), N 29.

C. Rechtliche Einordnung der automatisierten Gesichtserkennung

I. Schwere Grundrechtseingriffe

Automatisierte Gesichtserkennungssysteme verarbeiten Gesichtsmarkmale natürlicher Personen zu maschinenlesbaren Templates in Form von Datensätzen. Mit diesem technischen Vorgang werden aus den biometrischen Gesichtsmarkmalen biometrische Daten erstellt. Gemäss revidierter Datenschutzgesetzgebung gelten sämtliche Daten, die eine natürliche Person eindeutig identifizieren, als biometrische Daten (Art. 5 lit. c Ziff. 4 revDSG). Die Botschaft präzisiert, dass es sich bei biometrischen Daten um Personendaten handelt, «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».³⁴ Dazu gehören ausdrücklich auch Gesichtsbilder.³⁵ Dabei gilt es zu beachten, dass nicht jeder Umgang mit Gesichtsbildern eine biometrisch-technische Verarbeitung von Gesichtsmarkmalen darstellt. Der biometrisch relevante Datenverarbeitungsvorgang besteht aus der technischen Analyse entsprechender Merkmale und der Erstellung der Templates, welche abgeglichen werden. Gesichtserkennungssoftware generiert im Rahmen eines solchen «spezifischen technischen Verfahrens» aus «gewöhnlichen» Gesichtsbildern einer natürlichen Person Daten, die durch einen Abgleich eine eindeutige Identifizierung dieser Person ermöglichen (sollen).³⁶ Kommt Gesichtserkennungssoftware zum Einsatz, werden also biometrische Daten erstellt und bearbeitet.

Biometrische Datenbearbeitungsprozesse berühren Grundrechte betroffener Personen in besonderer Weise. Biometrische Daten werden in Art. 5 lit. c Ziff. 4 revDSG als besonders schützenswerte Personendaten qualifiziert, womit ein bis anhin geltender Grundsatz explizit im Gesetz verankert wurde.³⁷ Art. 13 Abs. 2 BV schützt vor jedem staatlichen Umgang mit personenbezogenen Daten,³⁸ wobei für die Beurteilung der Schwere eines entsprechenden Grundrechtseingriffs die konkrete Art der Bearbeitung sowie die von ihr betroffenen Daten massgeblich sind. Die Bearbeitung besonders schützenswerter Daten durch

34 BBl 2017 6941, 7020.

35 BBl 2017 6941, 7020.

36 Vgl. BEAT RUDIN, in: Bruno Baeriswyl/Kurt Pärli/Dominika Blonski (Hrsg.), Datenschutzgesetz, Stämpfli Handkommentar, 2. Aufl., Bern 2023, Art. 5 DSG N 31.

37 So bereits BLONSKI (Fn. 11), S. 57 f.; siehe auch FRANZISKA SPRECHER, Datenschutz und Big Data im Allgemeinen und im Gesundheitsrecht im Besonderen, ZBJV 2018, S. 482–552, S. 494.

38 RAINER J. SCHWEIZER, in: Bernhard Ehrenzeller et al. (Hrsg.), Die Schweizerische Bundesverfassung, St. Galler Kommentar, 3. Aufl., Zürich 2014, Art. 13 BV N 74; REGINA KIENER/WALTER KÄLIN/JUDITH WYTENBACH, Grundrechte, 3. Aufl., Bern 2017, § 14 N 57; vgl. Art. 34 Abs. 2 revDSG.

den Staat fällt in den Schutzbereich von Art. 13 Abs. 2 BV und gilt allgemein als schwerer Eingriff.³⁹ Kein schwerwiegender Eingriff wäre anzunehmen bei einer herkömmlichen (manuellen) Bearbeitung von Fotografien ohne Beizug von Gesichtserkennungssoftware.⁴⁰ Die Generierung und Bearbeitung biometrischer Informationen stellen hingegen einerseits aufgrund des besonderen Schutzes dieser Daten einen schweren Eingriff dar.⁴¹ Andererseits spricht auch die automatisierte und systematische (Massen-)Bearbeitung und die damit deutlich erweiterten Möglichkeiten der Datenbearbeitung für die Klassifikation als schwerwiegender Eingriff in Art. 13 Abs. 2 BV.

Mit dem ersten Schritt der automatisierten Gesichtserkennung, der maschinellen Generierung der Templates, werden aus den Gesichtern der erfassten Personen biometrische Daten erstellt. Es erfolgt ein erster schwerer Grundrechtseingriff, und zwar gegenüber allen Personen, deren Gesichter in den Erkennungsprozess einbezogen und damit vermessen werden. Betroffen ist nicht nur die eigentliche «Zielperson», sondern sind dies auch sämtliche Personen, deren Gesichter zwecks Abgleichs erfasst und in Templates verarbeitet werden. Im Anschluss an die Extraktion der Templates erfolgt ein Abgleich dieser Daten, womit biometrische Daten nicht nur generiert, sondern auch weiterverwendet werden. Mit dem Abgleich wird ein zweites Mal schwer in die Grundrechte all derjenigen Personen eingegriffen, deren Daten für den Abgleich verwendet werden. Von den beiden Grundrechtseingriffen betroffen sind auch «Nicht-Treffer», d.h. diejenigen Personen, die zum Zweck des Abgleichs erfasst, aber aufgrund fehlender Übereinstimmung nicht identifiziert werden. So bestätigt die bundesgerichtliche Rechtsprechung⁴² (wie auch diejenige des Deutschen Bundesverfassungsgerichts⁴³), dass die automatisierte Erfassung eines Kennzeichens und dessen Abgleich mit einer Datenbank einen Grundrechtseingriff darstellt, und zwar auch dann, wenn dies nicht zu einem Treffer führt.

Es ist festzuhalten, dass von der automatisierten Gesichtserkennung nicht nur einzelne Tatverdächtige betroffen sind, sondern auch eine grosse Zahl unbeteiligter Personen, deren Gesichter zum Zweck des Abgleichs biometrisch erfasst und für den Datenabgleich verwendet werden, sei dies, weil sie im Bild- oder Videomaterial (1:n-Abgleich) ebenfalls zu sehen sind oder weil sie in polizeilichen Datenbanken (n:1-Abgleich) erfasst sind.

Eingriffe in Grundrechte bedürfen einer gesetzlichen Grundlage, schwere Eingriffe erfordern eine Grundlage im formellen Gesetz (Art. 36 Abs. 1 BV).⁴⁴ Das zweigliedrige technische Verfahren der automatisierten Gesichtserkennung führt zu zwei Grundrechtseingriffen, die separat zu werten sind. Die Vermes-

39 SCHWEIZER (Fn. 38), Art. 13 BV N 77.

40 Vgl. RUDIN (Fn. 36), Art. 5 DSGVO N 31.

41 BLONSKI (Fn. 11), S. 69; vgl. auch Art. 34 Abs. 2 revDSG.

42 BGer 1C_39/2021 v. 29.11.2022, E. 8.10.2.

43 BVerfG 150, 244 (KfZ-Kennzeichen II).

44 SCHWEIZER (Fn. 38), Art. 36 BV N 16.

sung vieler Gesichter als Massnahme mit grosser Streubreite bedarf einer ausreichend bestimmten formell-gesetzlichen Grundlage. Für den Abgleich solcher Daten mit rechtmässig erhobenen Datenquellen oder Datenbanken ist eine solche ebenfalls notwendig.

II. Strafprozessuale Zwangsmassnahme

Strafverfahren können mit einschneidenden Grundrechtseingriffen einhergehen. Eingriffe in grundrechtlich geschützte Positionen, welche betroffene Personen zur Durchführung eines Strafverfahrens über sich ergehen lassen müssen, werden als Zwangsmassnahmen bezeichnet.⁴⁵ Gemäss Art. 196 StPO sind Zwangsmassnahmen sämtliche Verfahrenshandlungen der Strafbehörden, die in Grundrechte der Betroffenen eingreifen und dazu dienen, Beweise zu sichern (lit. a), die Anwesenheit von Personen im Verfahren sicherzustellen (lit. b) oder die Vollstreckung des Entscheides zu gewährleisten (lit. c).

Beim Einsatz automatisierter Gesichtserkennung steht die Beweissicherung nach lit. a im Vordergrund, soll doch durch die biometrische Analyse eine Person zum Zwecke eines Tatnachweises identifiziert werden.⁴⁶ Entsprechend ist KÜHNE zu widersprechen, dass der automatisierte Vorgang keinen der in Art. 196 StPO genannten Zwecke verfolgt. Zwangsmassnahmen, die der konkreten Beweisführung dienen, fallen unter Art. 196 lit. a StPO. Diese Einordnung der automatisierten Gesichtserkennung zu Ermittlungszwecken ergibt sich auch mit Blick auf die Parallelen zur DNA-Analyse.⁴⁷ Zwangsmassnahmen setzen ferner keinen physischen Zwang oder Widerstand voraus. Entscheidend ist die Qualität einer Massnahme als Eingriff in verfassungsmässige Rechte.⁴⁸ Der Einsatz automatisierter Gesichtserkennung bedingt schwere Eingriffe in Art. 13 Abs. 2 BV und weist deshalb die für die Qualifikation als Zwangsmassnahme notwendige Eingriffsqualität auf. Art. 197 Abs. 1 lit. a StPO hält fest, dass Zwangsmassnahmen nur ergriffen werden dürfen, wenn sie formell-gesetzlich vorgesehen sind.⁴⁹

45 NIKLAUS SCHMID/DANIEL JOSITSCH, Handbuch des Schweizerischen Strafprozessrechts, 3. Aufl., Zürich/St. Gallen 2017, N 970 f.

46 A.M. KÜHNE (Fn. 2), S. 20.

47 Wie bei einer DNA-Analyse (Art. 255 ff. StPO) werden bei der Gesichtserkennung basierend auf biologischen Merkmalen Profile natürlicher Personen erstellt. Ziel einer DNA-Analyse ist die gegenseitige Zuordnung von tat- und täterbezogenen Spuren. Gesichtserkennung bezweckt die eindeutige Zuordnung von Gesichtsbildern zu Identitäten natürlicher Personen, womit genauso tatbezogene Spuren (z.B. Bild- oder Videomaterial des Tatgeschehens) täterbezogenen Elementen zugeordnet werden.

48 BBl 2006 1085, 1215; JONAS WEBER, in: Marcel A. Niggli/Marianne Heer/Hans Wiprächtiger (Hrsg.), Basler Kommentar StPO/JStPO, 2. Aufl., Basel 2014 (zit. BSK StPO), Art. 196 N 2 f.

49 Vgl. BSK StPO-WEBER (Fn. 48), Art. 197 N 4; SVEN ZIMMERLIN, in: Andreas Donatsch et al. (Hrsg.), Kommentar zur Schweizerischen Strafprozessordnung, 3. Aufl., Zürich 2020 (zit. SK-Komm.), Art. 197 StPO N 2.

III. Qualifizierte Datenanalyse

An Eingriffe in Art. 13 Abs. 2 BV sind hohe Anforderungen gestellt. In jüngerer Zeit wurde dies insbesondere bei der bundesgerichtlichen Rechtsprechung zu den polizeigesetzlichen Grundlagen der AFV in den Kantonen Thurgau und Solothurn deutlich.⁵⁰ Gemäss Bundesgericht sind automatisierte Überwachungs-, Fahndungs- und Datenbearbeitungssysteme wie eine systematische Erfassung von Kontrollschildern durch Kameras mit einer massenhaften und praktisch unbegrenzten Erhebung und Auswertung von Daten verbunden und folglich als schwere Grundrechtseingriffe einzustufen.⁵¹ Die hohe Intensität ergebe sich durch die serielle und simultane Verarbeitung grosser Datensätze sowie der Möglichkeit, die Daten mit anderen zu kombinieren.⁵² Das Bundesgericht erachtet somit die Automatisierung solcher Abgleiche als Faktor, der die Eingriffsintensität erhöht. Bei automatisierten Datenabgleichen sei nicht nur die Erhebung der Daten, sondern auch jeder weitere Datenbearbeitungsschritt gesetzlich vorzusehen.⁵³ Es müsse erkennbar sein, ob und mit welchen Daten ein allfälliger Datenabgleich erfolgt. Unter anderem ist der Katalog an Daten, mit denen der Abgleich erfolgt, mit genügender Bestimmtheit zu regeln und die Reichweite des Abgleichs im Gesetz selbst sachbezogen einzugrenzen.⁵⁴

Für die automatisierte Gesichtserkennung bedeutet dies, dass alle Datenbearbeitungsschritte, die jeweils eigens für sich Grundrechte berühren, genügend bestimmt gesetzlich zu regeln sind. Digitale Ermittlungen können allgemein in drei Schritte unterteilt werden: (1.) Datenbeschaffung, (2.) Datenanalyse und (3.) Datenverwertung. Bezüglich des Verfahrens, dessen sich die automatisierte Gesichtserkennung bedient, wurde bereits sichtbar, dass der erste Schritt in der Beschaffung von Gesichtsbildern besteht. Diese Datenbeschaffung ist Vorbedingung jeder Gesichtsanalyse. Wird an öffentlichen Plätzen videoüberwacht oder ein Smartphone beschlagnahmt, ist für die Beschaffung dieser Daten durch Strafverfolgungsbehörden eine Rechtsgrundlage erforderlich. Das Verständnis von strafprozessualen Zwangsmassnahmen aber auch weiteren Untersuchungshandlungen wie bspw. ein Aktenbeizug fokussiert traditionell auf die Beschaffung von Daten.

Die Annahme, dass nur die ursprüngliche erste Beschaffung von Daten grundrechtsrelevant ist und der Staat in der Folge mit den Daten machen kann, was er möchte, widerspricht der erwähnten Rechtsprechung. Auch die ausführliche Regulierung der Analyse von DNA zeigt, dass sich die Normen nicht nur

50 BGE 146 I 11; BGer 1C_39/2021 v. 29.11.2022.

51 So in Bezug auf die AFV BGer 1C_39/2021 v. 29.11.2022, E. 8.1.1.

52 BGer 1C_39/2021 v. 29.11.2022, E. 8.1.1

53 BGE 146 I 11, E. 3.3.2.

54 BGE 146 I 11, E. 3.3.2; BGer 1C_39/2021 v. 29.11.2022, E. 8.5.1.

auf die Datenbeschaffung zu beschränken haben.⁵⁵ Die Annahme ist auch schlicht nicht mehr zeitgemäss, missachtet sie doch die grundrechtlich potenziell hohe Relevanz weitergehender Datenbearbeitungen. Mit avancierten technischen Analysen können aus Ausgangsdaten neue Informationsgehalte extrahiert werden.⁵⁶ Das zeigt sich eindrücklich an der automatisierten Gesichtserkennung als qualifizierte Art der Datenanalyse. Als biometrische Analyse vermisst sie Abbilder in einer Weise, die in der Folge eine eindeutige Identifizierung zulassen (sollen).⁵⁷ Diese Vermessung schafft Daten neuer Qualität. So sind z.B. auch das Vorhandensein eines Bildes von einem Finger und die hochpräzise automatisierte Vermessung eines Fingerabdrucks qualitativ zwei verschiedene Dinge. Solche Datenanalysen könnten ebenfalls als Datenbeschaffungen verstanden werden, da dem Staat neue Daten, d.h. neue Informationen zugänglich werden. Nicht nur das Erlangen des Bildmaterials, sondern auch das Erstellen der Gesichtstemplates ist deshalb als eigenständige Datenbearbeitung gesetzlich vorzusehen. Das gilt auch für die darauffolgende Analyse i.e.S., welche mit dem Abgleich der Daten erfolgt. In diesem letzten Schritt werden Datensätze miteinander verknüpft, womit weitere Informationen über Individuen beschafft werden können. Welche Daten mit welchen Datensätzen abgeglichen werden dürfen, ist folglich ebenfalls gesetzlich einzugrenzen.⁵⁸ Werden die Templates oder Resultate des Datenabgleichs in der Folge nochmalig weiterverwendet, z.B. in eine Datenbank eingespeist, aufbewahrt oder an andere Behörden weitergegeben, ist schliesslich auch diese Datenverwertung im Gesetz vorzusehen.⁵⁹

Die biometrische Erfassung und der Abgleich heben sich qualitativ deutlich von manuellen Sichtungen von Bild- und Videomaterial ab, z.B. durch sog. Super-Recognizer⁶⁰. Die manuelle Sichtung geht nicht nur nicht mit der Erstellung biometrischer Datensätze einher, sondern ist auch bezüglich Streubreite weniger invasiv, d.h. die Zahl von der Bearbeitung betroffener Personen ist deutlich tiefer. Die Reichweite der automatisierten Gesichtserkennung ist viel grösser, als dies bei einer manuellen Sichtung je möglich wäre. Die Argumentation, dass es keinen Unterschied mache, ob die Daten durch Mensch oder Maschine gesichtet werden,⁶¹ schlägt deshalb fehl.

55 Vgl. NIKLAUS OBERHOLZER, Grundzüge des Strafprozessrechts, 4. Aufl., Bern 2020, N 1465 ff.; SCHMID/JOSITSCH (Fn. 45), N 1090 ff.

56 Vgl. HUPONT et al. (Fn. 9), S. 1.

57 Dazu schon Kap. C.I.

58 BGE 146 I 11, E. 3.3.2; BGer 1C_39/2021 v. 29.11.2022, E. 8.5.1.

59 BGer 1C_39/2021 v. 29.11.2022, E. 8.9.2.

60 Dazu NZZ vom 01.01.2023, «Sie erkennen Gesichter besser als jede Software: Erstes Schweizer Polizeikorps setzt auf Super-Recognizer».

61 So die Argumentation der Kantonspolizei St. Gallen in KARABOGA et al. (Fn. 4), S. 120 f.

D. StPO-Roulette: Findet sich eine rechtliche Grundlage?

Im Nachgang zu unserer ersten Publikation wurde über die Rechtmässigkeit der automatisierten Gesichtserkennung viel debattiert. BRAUN BINDER/KUNZ/OBRECHT widmeten sich dem Einsatz maschineller Gesichtserkennung im öffentlichen Raum und verneinten dessen Rechtmässigkeit in Übereinstimmung mit uns. KÜHNE untersuchte im Rahmen einer Replik die automatisierte Bearbeitung von Personendaten im Strafprozess und erachtete diese im Gegensatz zu uns als zulässig (Kap. A). Im September 2021 richtete Nationalrätin RINIKER Fragen bzgl. allfällig notwendiger Gesetzesrevisionen an den Bundesrat. Der Bundesrat antwortete, dass gestützt auf die existierenden Rechtsgrundlagen biometrische Gesichtsdaten für die Identifizierung einer Person in Strafverfahren einsetzbar seien.⁶² Die rechtlichen Grundlagen wurden vom Bundesrat nicht benannt. Kürzlich wurde deshalb eine weitere Interpellation von Nationalrätin MARTI zur automatisierten Gesichtserkennung in Strafverfahren eingereicht, bei deren Beantwortung der Bundesrat zu den Rechtsgrundlagen Stellung bezieht.⁶³ In der weiteren öffentlichen Debatte wurden über diverse Kanäle⁶⁴ verschiedenste Normen als rechtliche Grundlagen vorgeschlagen. Die Vorschläge gleichen in der Gesamtheit beinahe einem «StPO-Roulette», bei dem das Kügelchen zufällig auf unterschiedlichen StPO-Normen zur Rechtfertigung des Einsatzes zu liegen kommt. Diesen herangezogenen Rechtsgrundlagen wollen wir uns trotzdem im Einzelnen widmen, um anhand einer vertieften Auseinandersetzung aufzuzeigen, weshalb sie als gesetzliche Grundlagen für den Einsatz automatisierter Gesichtserkennung im Strafverfahren nicht ausreichen.

I. Art. 260 f. StPO

KÜHNE begründet die Rechtmässigkeit der automatisierten Gesichtserkennung im Strafverfahren im Wesentlichen mit Art. 260 StPO. Die Norm zur ED-Erfassung bilde die gesetzliche Grundlage für den Datenabgleich, welcher im Rahmen des Gesichtserkennungsverfahrens stattfindet.⁶⁵ Art. 260 StPO sieht in Abs. 1 vor, dass die Körpermerkmale einer Person festgestellt und Abdrücke von Körperteilen genommen werden können. Gemäss KÜHNE fällt darunter auch die Fotografie des Gesichts sowie dessen Vermessung. Der anschliessende

62 Frage Riniker 21.7896, «Gesichtserkennung zur Identifizierung im öffentlichen Raum».

63 Interpellation Marti 22.3993, «Rechtliche Grundlage für die automatisierte Gesichtserkennung in Strafverfahren».

64 So z.B. in Beiträgen auf LinkedIn, abrufbar unter: <https://www.linkedin.com/posts/monika-simmler-525ba815a_gesichtserkennung-%C3%BCberwachung-wieso-activity-6976047722608914433-3uy3/?originalSubdomain=ch> (26.05.2023) oder in Medienberichten wie SRF Schweiz Aktuell vom 14.09.2022 «St. Gallen will Gesichtserkennung im öffentlichen Raum verbieten» und in der SRF Rundschau (Fn. 3).

65 KÜHNE (Fn. 2), S. 22.

Abgleich der so erhobenen Daten stelle den Sinn der ED-Erfassung dar und sei deshalb erlaubt.⁶⁶

Die ED-Erfassung beschränkt sich auf die Feststellung von äusserlich wahrnehmbaren Tatsachen, wie etwa Grösse, Aussehen, Gewicht, Abdrücken von Fingern, Handballen, Ohren, Füßen oder Zähnen.⁶⁷ Bei der automatisierten Gesichtserkennung werden die Gesichtsm Merkmale einer Person allerdings vermessen und zu biometrischen Daten verarbeitet, um sie in der Folge einem Abgleich zu unterziehen. Diese Weiterbearbeitung von «Gesichtsabdrücken» lässt sich aus dem Normtext nicht ableiten. In den Materialien zu Art. 260 f. StPO wurde die Vermessung von Gesichtern nicht erwähnt.⁶⁸ Dennoch könnte angenommen werden, dass die biometrische Vermessung der Gesichtsm Merkmale von einer ED-Erfassung umfasst wird.⁶⁹ In diesem Fall würde mit Art. 260 StPO eine Grundlage für die Erfassung des Gesichts der zu identifizierenden Person vorliegen. Auch dann würde die Norm allerdings nur einen Bruchteil des Prozesses abdecken, der für die automatisierte Gesichtserkennung notwendig ist.

Art. 260 StPO ist als Rechtsgrundlage für die automatisierte Gesichtserkennung aus mehreren Gründen unvollkommen. Bei der ED-Erfassung handelt es sich um eine Zwangsmassnahme, deren Anordnung eines hinreichenden Tatverdachts bedarf (Art. 197 Abs. 1 lit. b StPO).⁷⁰ Eine ED-Erfassung muss gemäss Art. 260 Abs. 3 StPO schriftlich verfügt und kurz begründet werden. Angeordnet werden kann sie nicht nur gegenüber beschuldigten Personen, sondern auch gegenüber Dritten.⁷¹ Weil bei der Anordnung von Zwangsmassnahmen gegenüber nicht beschuldigten Personen besondere Zurückhaltung geboten ist (Art. 197 Abs. 2 StPO), erfordert die Anordnung der ED-Erfassung nicht beschuldigter Personen eine besondere Begründung.⁷² Die Crux der automatisierten Gesichtserkennung liegt darin, dass nicht nur die Gesichter einzelner Personen, sondern einer Vielzahl von Personen biometrisch erfasst werden, damit der Datenabgleich stattfinden kann. Werden Tausende Smartphone-Fotos oder Videoüberwachungsaufnahmen analysiert, wird eine unbestimmte Zahl *n* nicht verfahrensbeteiligter Dritter biometrisch analysiert.⁷³ Diese biometrische Erfassung einer Vielzahl nicht beschuldigter Personen kann gestützt auf Art. 260 StPO nicht gerechtfertigt werden. Art. 260 StPO ist offensichtlich nicht auf eigentliche Massen-ED-Erfassungen ausgerichtet. Die schriftliche Anordnung

66 KÜHNE (Fn. 2), S. 22.

67 BB1 2005 1085, 1243.

68 BB1 2005 1085, 1243.

69 So i.E. KÜHNE (Fn. 2), S. 22; in diese Richtung auch BSK StPO-WERLEN (Fn. 48), Art. 260 N 1 sowie SK-Komm.-GRAF/HANSJAKOB (Fn. 49), Art. 260 StPO N 1.

70 SK-Komm.-GRAF/HANSJAKOB (Fn. 49), Art. 260 StPO N 5.

71 BB1 2006 1085 1243; SK-Komm.-GRAF/HANSJAKOB (Fn. 49), Art. 260 StPO N 5.

72 SK-Komm.-GRAF/HANSJAKOB (Fn. 49), Art. 260 StPO N 7a.

73 Zu den Varianten Kap. B.III.

der Zwangsmassnahme gegenüber allen betroffenen Personen wäre zudem nicht praktikabel, müsste sie doch lauten «alle n Personen, die möglicherweise in den Aufnahmen gefunden werden, werden erkennungsdienstlich erfasst». Eine solche Anordnung wäre reichlich unbestimmt.

Als weiteres Argument tritt hinzu, dass der zweite Schritt der automatisierten Gesichtserkennung, der Abgleich bzw. die Analyse i.e.S. selbst, von Art. 260 StPO auch mit grosszügigster Auslegung nicht angesprochen ist. Einzig ein Abgleich eines Beschuldigten 1 mit bereits in der ED-Datenbank erfassten Gesichtern n könnte allenfalls als «Weiterverwendung» von ED-Unterlagen i.S.v. Art. 261 StPO verstanden werden. Art. 261 StPO erlaubt die Aufbewahrung und Verwendung von ED-Daten unter gewissen Voraussetzungen. Die Verwendung zwecks automatisierter Gesichtserkennung würde jedoch voraussetzen, dass alle in der ED-Datenbank gespeicherten Gesichtsbilder biometrisch erfasst, d.h. rückwirkend Templates der Gesichter erstellt werden. Das würde einer erneuten, rückwirkenden ED-Erfassung gleichkommen. Das ist nicht Zweck von Art. 261 StPO. Für eine rückwirkende biometrische Erfassung besteht keine Rechtsgrundlage. Zudem wäre der nachfolgende Abgleich der erstellten biometrischen Daten auch hier gesetzlich nicht geregelt.

Die Art. 260 f. StPO vermögen Einsätze automatisierter Gesichtserkennung nicht abzudecken. Nicht hinreichend bestimmt (respektive überhaupt nicht) vorgesehen wird in Art. 260 f. StPO die biometrische Erfassung aller betroffenen Personen zwecks Abgleichs sowie der Abgleich der biometrischen Daten selbst.

II. Art. 95 ff. StPO

Subsidiär führt KÜHNE in seiner Replik Art. 95 ff. StPO als Rechtsgrundlage für den automatisierten Datenbearbeitungsvorgang an.⁷⁴ Mit Art. 95 ff. StPO werden grundlegende Prinzipien des Datenschutzrechts in die StPO übernommen.⁷⁵ Diese allgemeinen Grundsätze beziehen sich auf die Beschaffung und Bearbeitung von Daten im Zuge hängiger Strafverfahren.⁷⁶

Teilweise wird Art. 95 StPO von Strafverfolgungsbehörden als gesetzliche Grundlage zur Datenbearbeitung herangezogen, so für das «Googeln» durch Behörden⁷⁷ oder, wie eben durch KÜHNE, für die Bearbeitung von Daten Dritter.⁷⁸ Ein Teil der Lehre stützt diese Annahme, wenn auch nur in beschränktem

74 KÜHNE (Fn. 2), S. 21, der in Art. 95 StPO die rechtliche Grundlage für Datenbearbeitungen gegenüber nicht beschuldigten Personen sieht.

75 BSK StPO-FIOLKA (Fn. 48), Vor Art. 95 N 1; BB1 2006 1085, 1159.

76 BSK StPO-FIOLKA (Fn. 48), Vor Art. 95 N 2.

77 ANNA CARTNER/SANDRA SCHWEINGRUBER, Strafbehörden dürfen googeln, AJP 2021, S. 990–998, S. 993 f.

78 KÜHNE (Fn. 2), S. 22.

Masse.⁷⁹ Art. 95 StPO normiert streng genommen nur den Grundsatz und die Pflicht transparenter Datenbeschaffung,⁸⁰ äussert sich aber nicht dazu, zu welchem Zweck, unter welchen Umständen und von welchen Personen Daten beschafft werden dürfen. Art. 95 StPO kann deshalb nicht als Blankett-Norm zur Rechtfertigung sämtlicher Datenbearbeitungen, welche im Rahmen eines Strafverfahrens anfallen und technisch möglich wären, herangezogen werden, schon gar nicht für Zwangsmassnahmen.

Schwerwiegende Eingriffe in Art. 13 Abs. 2 BV bedürften gemäss Bundesgericht einer gesetzlichen Grundlage, die präzise umschreibt, welche Daten für welche Zwecke bearbeitet werden.⁸¹ Zur Rechtfertigung der Bearbeitung von besonders schützenswerten Personendaten, Datenbearbeitungen mit einer gewissen Streuweite und automatisierten Verknüpfungen sowie Abgleichen mit anderen Datensätzen ist Art. 95 StPO zu unbestimmt.⁸² Art. 95 StPO präzisiert in keiner Weise, welche Arten von Daten zu welchen Zwecken beschafft und bearbeitet werden können. Würde man Art. 95 StPO als ausreichend bestimmt für alle Datenanalysen der Strafverfolgungsbehörden erachten, auch für solche qualifizierter Art, bedeutete das, dass zu Ermittlungszwecken mit einmal erlangten Daten alles gemacht werden dürfte. Das steht im Widerspruch zur bundesgerichtlichen Rechtsprechung⁸³ und zu den Anforderungen an die Bestimmtheit von Normen⁸⁴. Schliesslich sei angemerkt, dass Art. 95 StPO gesetzssystematisch nicht als Zwangsmassnahme intendiert gewesen sein kann.

III. Art. 260 f. StPO i.V.m. Art. 354 StGB

Ein spezifischeres Gebilde an Rechtsgrundlagen bringt der Bundesrat in der Stellungnahme zur Interpellation 22.3993 von Nationalrätin MARTI vor.⁸⁵ Gemäss Bundesrat liegen mit Art. 260 f. StPO, Art. 354 Abs. 1 StGB sowie Art. 14 Abs. 2 des Bundesgesetzes über die polizeilichen Informationssysteme des Bundes (BPI) einschlägige gesetzliche Grundlagen für die Bearbeitung besonders schützenswerter Personendaten im Rahmen der Gesichtserkennung vor.

79 So z.B. BSK StPO-FIOLKA (Fn. 48), Art. 95 N 1, welcher in Art. 95 StPO eine allgemeine gesetzliche Grundlage für Datenbeschaffungen sieht, und SÉBASTIEN FANTI/SANDRINE ROHMER, in: Yvan Jeanneret/André Kuhn/Camille Perrier Depeursinge (Hrsg.), *Commentaire Romand, Code de procédure pénale suisse*, 2. Aufl., Basel 2019, Art. 95 N 21, gemäss welchen die Norm eine formell-gesetzliche Grundlage für Datenbeschaffungen darstellt, um bspw. allgemeine Informationen über Personen zu erlangen, nicht aber für systematische Datenabgleiche.

80 SK-Komm.-BRÜSCHWILER/GRÜNIG (Fn. 49), Art. 95 StPO N 3.

81 BGE 146 I 11, E. 3.3.1 f.

82 So bereits SIMMLER/CANOVA (Fn. 1), S. 114.

83 Dazu bereits ausführlich Kap. C.III.

84 KIENER/KÄLIN/WYTTEBACH (Fn. 38), § 9 N 53 und 56; SCHWEIZER (Fn. 38), Art. 36 BV N 23.

85 Interpellation 22.3993 (Fn. 63).

Begründet wird dies folgendermassen: Im Grundsatz handle es sich bei einem – manuellen oder automatisiert durchgeführten – Abgleich von Gesichtsbildern zur Identifikation von Personen schlicht um einen «Gesichtsbildabgleich», wobei dieser Begriff von der «Gesichtserkennung», bei der Gesichter in Echtzeit identifiziert werden, abzugrenzen sei. Im Strafverfahren durchgeführte «Gesichtsbildabgleiche» seien als Verwendung von ED-Daten erlaubt. Diese begriffliche Trennung zwischen Gesichtsbildabgleichen und Echtzeit-Gesichtserkennung überzeugt nicht. Der Modus des Datenabgleichs (Echtzeit oder nachträglich) ist zwar entscheidend für die Intensität der Massnahme, ändert aber nichts daran, dass nachträgliche Abgleiche genauso wie solche in Echtzeit Anwendungsformen der automatisierten Gesichtserkennung sind.⁸⁶

Warum die automatisierte Gesichtserkennung sich nicht auf Art. 260 f. StPO stützen kann, wurde bereits erläutert. Art. 354 Abs. 1 StGB erlaubt dem «zuständigen Departement» – gemeint ist damit das EJPD bzw. innerhalb diesem das Fedpol – allerdings die ihm übermittelten ED-Daten zu registrieren und zu speichern. Gestützt auf diese Bestimmung wird das automatische Fingerabdruck-Identifizierungssystem (AFIS) durch das Fedpol betrieben.⁸⁷ Aus dem Normtext und der systematischen Position der Norm im hinteren Teil des StGB (Titel «Amtshilfe im Bereich der Polizei», Marginalie «Zusammenarbeit bei der Identifizierung von Personen») ergibt sich nicht nur, dass diese Rechtsgrundlage nur Datenbearbeitungen durch das EJPD bzw. das Fedpol umfasst, sondern auch, dass diese Norm eine Grundlage zum organisatorischen Vorgehen bei Datenbearbeitungen darstellt, nicht jedoch eine für eigenständige Zwangsmassnahmen.

Wie der Bundesrat richtigerweise in der Stellungnahme ausführt, erlaubt Art. 354 Abs. 4 StGB i.V.m. Art. 2 lit. c der Verordnung über die Bearbeitung biometrischer ED-Daten (ED-Verordnung) dem Fedpol, ED-Daten inklusive Fotografien zu bearbeiten. Diese Daten können zur Identifizierung einer gesuchten oder unbekannten Person untereinander verglichen werden (Art. 354 Abs. 1 Satz 2 StGB). Der Bundesrat hält fest, dass die Kantone dem Fedpol gestützt auf Art. 354 Abs. 2 lit. d StGB (gemeint war wohl lit. g) entsprechende Daten zum Abgleich liefern dürfen. Dass das Fedpol erkennungsdienstliche Daten inklusive Fotografien bearbeiten darf, ergibt sich zusätzlich aus Art. 14 Abs. 2 BPI. Damit ist bereits gesagt, dass die Bearbeitung und der Abgleich von ED-Daten gestützt auf diese Rechtsgrundlagen nur durch die zuständige Behörde (ergo dem Fedpol selbst) erfolgen darf. Abgleiche von Gesichtsbildern, die von den kantonalen Polizeikörpern durchgeführt werden, sind von diesen Rechtsgrundlagen nicht erfasst. Die Benutzung von Gesichtserkennungs-

86 So auch die Einstufung von BRAUN BINDER/KUNZ/OBRECHT (Fn. 5), N 10 ff. sowie die Klassifikation von Gesichtserkennungssystemen in der KI-Verordnung, dazu HUPONT et al. (Fn. 9), S. 7.

87 MARCO GAMMA, in: Marcel A. Niggli/Hans Wiprächtiger (Hrsg.), Basler Kommentar StGB/JStG, 4. Aufl., Basel 2019, Art. 354 N 8 f.

software durch die Kantonspolizei St. Gallen⁸⁸ und die in der Öffentlichkeit⁸⁹ diskutierten Anwendungen involvieren das Fedpol allerdings nicht, können sich also nicht auf die vom Bundesrat vorgebrachten gesetzlichen Grundlagen stützen.

Im April 2023 kündigte der Bundesrat an, dass das AFIS mit dem Projekt AFIS2026 nun tatsächlich um ein Modul für einen «Gesichtsbildabgleich» erweitert werden soll.⁹⁰ Damit könne im Strafverfahren zukünftig ein Bild einer verdächtigen Person mit im AFIS gespeicherten ED-Bildern abgeglichen werden. Gemäss Medienmitteilung bestehen die Rechtsgrundlagen für solche Abgleiche bereits seit 2013. Ob die derzeit bestehenden Rechtsgrundlagen (Art. 354 StGB i.V.m. ED-Verordnung) für einen im Rahmen des AFIS durchgeführten Gesichtsbildabgleich ausreichen, bleibt in Anbetracht der geringen Bestimmtheit der Normen jedoch fraglich.

So erlaubt Art. 3 Abs. 1 lit. a i.V.m. Art. 2 lit. c ED-Verordnung dem Fedpol den automatisierten Abgleich und die Auswertung von biometrischen ED-Daten (inklusive Fotografien). Damit werden die Erfassung und der Abgleich von biometrischen Gesichtsmerkmalen zwar nicht ausdrücklich vorgesehen, aber aus der Verordnung wird erkennbar, dass im Rahmen des AFIS automatisierte Abgleiche von ED-Daten möglich sein sollen. Die Bestimmungen halten in allgemeiner Weise fest, dass die zuständigen Dienste vom Fedpol entsprechende Daten abgleichen, auswerten und speichern dürfen (Art. 2 f., Art. 7 f. und Art. 16 ED-Verordnung). Grosszügig ausgelegt könnte die automatisierte Gesichtserkennung im Strafverfahren von diesen Verordnungsbestimmungen erfasst sein. Erlaubt wären jedoch auch dann nur Abgleiche, die durch das Fedpol selbst durchgeführt werden und die sich auf ED-Daten des AFIS beschränken. Die Regelung lässt allerdings die in Anbetracht der Eingriffsintensität erforderliche Bestimmtheit und Normstufe vermissen. Bedenkt man die strengen bundesgerichtlichen Anforderungen bei der Regulierung automatisierter Datenbearbeitungen, reichen sie deshalb kaum aus. Es wäre präziser vorzusehen, welche Daten biometrisch analysiert und mit welchen Datenbanken automatisiert abgeglichen werden. Zudem regeln die bestehenden Rechtsgrundlagen nicht, inwiefern bereits gespeicherte ED-Fotografien rückwirkend biometrisch analysiert werden können, was für den nutzenbringenden Abgleich notwendig wäre.⁹¹ Es ist fraglich, ob die rückwirkende biometrische Vermessung der rund 400 000 in der ED-Datenbank erfassten Personen verhältnismässig ist und inwiefern eine (reichlich un-

88 KÜHNE (Fn. 2), S. 14 f.

89 SRF Rundschau (Fn. 3)

90 Medienmitteilung des Bundesrates vom 6. April 2023, «Bundesrat heisst Verpflichtungskredit zur Erneuerung des AFIS-Systems gut», abrufbar unter: <<https://www.fedpol.admin.ch/fedpol/de/home/aktuell/mm.msg-id-94141.html>> (26.05.2023).

91 Dazu bereits Kap. D.I.

bestimmte) Pauschalermächtigung auf Verordnungsstufe diese Eingriffe zu rechtfertigen vermag.⁹²

Art. 354 StGB und die ED-Verordnung halten somit die Rahmenbedingungen für biometrische Datenabgleiche durch das Fedpol fest. Die Rechtsgrundlagen weisen jedoch eine zu geringe Normdichte auf. Dazu kommt die nicht angemessene Normstufe. Die biometrische Erfassung von Gesichtern und der automatisierte Abgleich der biometrischen Daten müssten als schwere Eingriffe in Grundrechte für (potenziell) Betroffene aus dem Gesetz selbst zumindest erahnbar sein. Diesem Anspruch genügt das geltende Recht nicht.

IV. Art. 246 ff. StPO

Mit Art. 246 StPO wurde von KÜHNE eine weitere Rechtsgrundlage ins Spiel gebracht.⁹³ Im Anschluss an die rechtmässige Beschaffung von Bild- und Videomaterial mittels Hausdurchsuchungen (Art. 244 f. StPO), Editionsverfügungen (Art. 265 StPO) oder Aktenbeizug (Art. 194 StPO) könnten die Gesichtsbilddaten mit Gesichtserkennungssoftware gestützt auf Art. 246 StPO durchsucht und entweder mit ED-Daten abgeglichen oder auf eine Übereinstimmung mit einer bestimmten Person X hin analysiert werden.⁹⁴

Die Durchsuchung i.S.v. Art. 246 StPO dient dazu, die Beweiseignung von Aufzeichnungen zu prüfen.⁹⁵ Diese Massnahme ist einer allfälligen Beschlagnahme vorgelagert und ermöglicht es, Aufzeichnungen und Datenträger vorab zu durchsuchen, um abzuklären, ob sich in den Aufzeichnungen Informationen befinden, die der Beschlagnahme unterliegen.⁹⁶ Dies entspricht vom Vorgehen und Zweck her nicht dem Verfahren der automatisierten Gesichtserkennung. Der Beizug von Gesichtserkennungstechnologie dient nicht dazu, Aufzeichnungen in Form von Bild- und Videodaten zu «sichten», um zu überprüfen, ob diese als Beweismittel beschlagnahmt werden können. Die Gesichtsbilddaten wurden in einem vorgelagerten Schritt bereits beschafft.

Zudem würde mit einer Subsumtion der automatisierten Gesichtserkennung unter Art. 246 StPO ausser Acht gelassen, dass damit biometrische Daten erstellt und abgeglichen werden. Das relevante Bild- und Videomaterial wird nicht nur «durchsucht», sondern aus den darin enthaltenen Gesichtern werden biometrische Templates extrahiert. Im Unterschied zu einer Objekterkennung,

92 Laut Fedpol sind in der nationalen Datenbank per 15. Januar 2023 insgesamt 1 012 810 Gesichtsbilder aus 387 181 erkennungsdienstlichen Behandlungen gespeichert, siehe «Gesichtsbildabgleich in Zahlen», abrufbar unter: <https://www.fedpol.admin.ch/fedpol/de/home/sicherheit/personenidentifikation-neu/gesichtsbildabgleich/zahlen.html> (26.05.2023).

93 KÜHNE (Fn. 2), S. 20.

94 KÜHNE (Fn. 2), S. 20.

95 SK-Komm.-KELLER (Fn. 49), Art. 246 StPO N 1; vgl. BSK StPO-THORMANN/BRECHBÜHL (Fn. 48), Art. 246 N 4.

96 SK-Komm.-KELLER (Fn. 49), Art. 246 StPO N 1; OBERHOLZER (Fn. 55), N 1406.

mit der analysiert wird, ob im Datenmaterial menschliche Gesichter enthalten sind, extrahiert Gesichtserkennungssoftware biometrische Merkmale. Dadurch werden Daten in neuer Qualität geschaffen.⁹⁷ Bei einer herkömmlichen Durchsuchung hingegen werden die ursprünglichen Daten zur Erhaltung der Beweiskette gerade nicht verändert oder weiterbearbeitet.⁹⁸ Wie z.B. bei der Nutzung der Suchfunktion des Word-Programms werden Aufzeichnungen lediglich nach bestimmten Elementen durchsucht, was deutlich weniger invasiv ist als die Erstellung biometrischer Gesichtsprofile. Die Qualifikation als Durchsuchung i.S.v. Art. 246 StPO würde dem Wesenskern der Gesichtserkennungstechnologie nicht gerecht.

V. Art. 260 ff. i.V.m. Art. 139 Abs. 1 StPO

In der anhaltenden Debatte wurde des Weiteren Art. 260 ff. i.V.m. Art. 139 Abs. 1 StPO als mögliche Rechtsgrundlage erwähnt.⁹⁹ Die entsprechende Argumentation lautet dahingehend, dass es rechtlich irrelevant sei, wie einmal beschaffte Bild- und Videodaten ausgewertet werden, solange die Daten rechtmässig beschafft wurden.¹⁰⁰ Das technische Vorgehen habe sich i.S.v. Art. 139 Abs. 1 StPO am Stand der Wissenschaft zu orientieren, was auch moderne Datenanalysen beinhalte.¹⁰¹ Diese Argumentation verkennt, dass mit der automatisierten Gesichtserkennung eine qualifizierte Datenanalyse erfolgt, die verschiedene Datenbearbeitungsschritte mit zusätzlichen Grundrechtseingriffen involviert.¹⁰² Auch wenn Bild- oder Videomaterial sowie die ED-Daten aller Beteiligten (1 und n) rechtmässig beschafft wurden, lässt sich eine nachgelagerte Datenanalyse mittels Gesichtserkennungssoftware nicht auf die Rechtsgrundlagen der Datenbeschaffung stützen. Das Erfordernis einer gesetzlichen Grundlage für jede weitere Verwendung der Daten ergibt sich aus der bundesgerichtlichen Rechtsprechung zur AFV.¹⁰³

Der erwähnte Art. 139 Abs. 1 StPO kann für selbstständige Zwangsmassnahmen allgemein nicht herangezogen werden. Die Norm bezieht sich auf die Beweiseignung und hält fest, dass die Strafbehörden zur Wahrheitsfindung alle nach dem Stand von Wissenschaft und Erfahrung geeigneten Beweismittel einsetzen dürfen, setzt aber gleichzeitig voraus, dass die Beweismittel selbst recht-

97 Dazu bereits Kap. C.III.

98 Vgl. SK-Komm.-KELLER (Fn. 49), Art. 247 StPO N 3a.

99 So die Argumentation eines Vertreters eines Forensischen Instituts zu einem Beitrag zur Gesichtserkennung auf LinkedIn (Fn. 64).

100 Vgl. dazu auch die von der Kantonspolizei St. Gallen vorgebrachte Argumentation in KARA-BOGA et al. (Fn. 4), S. 120 f.

101 So z.B. im Beitrag auf LinkedIn (Fn. 64).

102 So in Bezug auf die Videoüberwachung auch LUCIEN MÜLLER, Videoüberwachung in öffentlich zugänglichen Räumen – insbesondere zur Verhütung und Ahndung von Straftaten, Diss. Zürich/St. Gallen 2011, S. 130 f.

103 Dazu bereits Kap. C.III.

lich zulässig sein müssen. Wird mit der Beweisgewinnung in Grundrechte eingegriffen, bedarf dies einer eigenständigen gesetzlichen Grundlage.¹⁰⁴

VI. Art. 141 Abs. 2 StPO

Schliesslich führte KÜHNE Art. 141 Abs. 2 StPO als Argument für die Rechtmässigkeit an. Selbst wenn die automatisierte Gesichtserkennung im Strafverfahren widerrechtlich erfolge, «würde dies nicht per se zur Unverwertbarkeit der so erlangten Beweise führen», so KÜHNE.¹⁰⁵ Bei widerrechtlichen Datenbearbeitungen müsse in Anwendung von Art. 141 Abs. 2 StPO ohnehin eine Interessensabwägung vorgenommen werden. Bei schweren Straftaten sei das Ergebnis der Gesichtserkennungsanalyse als Beweis deshalb verwertbar, auch wenn deren Einsatz ohne rechtliche Grundlagen erfolge.¹⁰⁶ Diese Argumentation eines Behördenvertreters verblüfft. Würden wir ihr im Strafverfahren folgen, wäre dies rechtsstaatlich höchst problematisch.

Der materiellen Wahrheitsfindung werden mit Beweisverwertungsverböten Grenzen gesetzt.¹⁰⁷ Neben einem absoluten Beweisverwertungsverbot (Art. 140 i. V. m. Art. 141 Abs. 1 StPO) sieht die StPO ein relatives Beweisverwertungsverbot (Art. 141 Abs. 2 StPO) vor. Beweise, die in strafbarer Weise oder unter Verletzung von Gültigkeitsvorschriften erhoben wurden, dürfen nicht verwertet werden, es sei denn, ihre Verwertung sei zur Aufklärung schwerer Straftaten unerlässlich (Art. 141 Abs. 2 StPO). Um das Verwertungsverbot zu relativieren, muss stets eine Interessenabwägung zwischen dem öffentlichen Interesse an der Strafverfolgung und dem Interesse der betroffenen Personen an der Einhaltung der Verfahrensrechte erfolgen.¹⁰⁸ Beweise, die ohne hinreichend bestimmte gesetzliche Grundlage erhoben werden, gelten als rechtswidrig erhoben i. S. v. Art. 141 Abs. 2 StPO.¹⁰⁹ Diese Bestimmung darf jedoch keinesfalls «ersatzweise» als gesetzliche Grundlage für unrechtmässige Ermittlungsmethoden herangezogen werden. Auf sie darf nur in unumgänglichen Einzelfällen zurückgegriffen werden. Die Nutzung automatisierter Gesichtserkennung im Strafverfahren erfolgt institutionalisiert und voraussehbar. Bereits die Anschaffung von Gesichtserkennungstechnologie durch Behörden bringt zum Ausdruck, dass diese zukünftig zum Einsatz kommen soll. Ihr Einsatz stellt daher keinen unvorhergesehenen Ausnahmefall dar, welcher eine ausnahmsweise Verwertung legitimieren könnte. Gesichtserkennungstechnologie vorsätzlich unrechtmässig zu verwenden mit Verweis auf Art. 141 Abs. 2 StPO läuft der *ratio legis* dieser Norm zuwider und ist nicht haltbar.

104 SK-Komm.-WOHLERS (Fn. 49), Art. 139 StPO N 4.

105 KÜHNE (Fn. 2), S. 23.

106 KÜHNE (Fn. 2), S. 23.

107 OBERHOLZER (Fn. 55), N 1093; SK-Komm.-WOHLERS (Fn. 49), Art. 141 StPO N 1.

108 OBERHOLZER (Fn. 55), N 1104 f.

109 BGE 146 I 11, E. 4.3, so auch KÜHNE (Fn. 2), S. 23.

Der Rückgriff auf Art. 141 Abs. 2 StPO als Rechtfertigungsgrundlage für den Einsatz automatisierter Gesichtserkennung im Strafverfahren impliziert des Weiteren geradezu, dass es sich dabei um eine unrechtmässige Beweiserhebungsmethode handelt, für die keine Rechtsgrundlage besteht. Die Rechtmässigkeit der automatisierten Gesichtserkennung mit einer Norm zur Verwertbarkeit rechtswidrig erlangter Beweise zu begründen, überzeugt nicht.

E. Synthese

Für Einsätze automatisierter Gesichtserkennung im Strafverfahren findet sich *de lege lata* keine gesetzliche Grundlage, welche dieses technische Verfahren in all seinen Bestandteilen abdeckt. Klarerweise zu unbestimmt für die Rechtfertigung von schweren Grundrechtseingriffen sind Art. 95 ff. StPO. Demgegenüber existieren mit Art. 246 ff., Art. 260 f. und Art. 263 ff. StPO einschlägige gesetzliche Grundlagen für die Beschaffung von Bild- und Videomaterial sowie von ED-Daten der zu identifizierenden Person. Diese Normen regeln jedoch nur (teilweise) die Beschaffung der nachfolgend analysierten und abgeglichenen Daten. Die Erstellung der Templates und insbesondere deren Datenabgleich ist nicht vorgesehen. Die Art. 260 f. StPO i.V.m. Art. 354 StGB und der ED-Verordnung sehen die Erfassung und den Abgleich von biometrischen Gesichtsmerkmalen in den Umrissen aber weder hinreichend bestimmt noch auf angemessener Normstufe vor. Nicht ermöglicht werden dadurch biometrische Datenabgleiche unter Verwendung von polizeieigenen Gesichtserkennungssystemen und Datenbanken der kantonalen Polizeikorps. Das Fazit unserer ersten Publikation kann deshalb bekräftigt werden: Der Einsatz automatisierter Gesichtserkennung durch kantonale Polizeikorps ist sicherlich unrechtmässig, derjenige durch das Fedpol mit hoher Wahrscheinlichkeit ebenso.

F. Regulierung der automatisierten Gesichtserkennung

Es ist am Gesetzgeber zu entscheiden, ob und ggf. wie er die automatisierte Gesichtserkennung im Strafverfahren für die Zukunft erlauben möchte. Die freiheitsrechtlichen Implikationen der Technologie, ihr Missbrauchspotenzial¹¹⁰ und ihre Weiterverwendungsmöglichkeiten z.B. im Rahmen der sog. Emotion Recognition¹¹¹ rechtfertigen eine gesellschaftspolitische Auseinandersetzung mit den Vor- und Nachteilen dieses Technologieeinsatzes. Im Strafverfahren

110 EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, Facial recognition technology: fundamental rights considerations in the context of law enforcement, Wien 2019, S. 9 ff.

111 LENA PODOLETZ, We have to talk about emotional AI and crime, AI & Society 2022.

sind sämtliche in Grundrechte eingreifende Verfahrenshandlungen verboten, sofern für sie keine Gesetzesgrundlage vorliegt. Die automatisierte Gesichtserkennung darf deshalb nicht zum Einsatz kommen bis der zu führende demokratische Diskurs ggf. in einem Gesetzgebungsverfahren resultierte. Möchte die Politik auf den Einsatz weiterhin verzichten, muss sie folglich nichts regulieren. Sollen *de lege ferenda* entsprechende Möglichkeiten für die Polizei geschaffen werden, bedürfte es hingegen neuer Normen.

I. KI-Verordnung der EU

Hinsichtlich einer möglichen Regulierung in der Schweiz lohnt sich ein Blick auf den Regulierungsvorschlag der EU für ein Gesetz über künstliche Intelligenz (KI-Verordnung).¹¹² Die KI-Verordnung verfolgt einen risikobasierten Ansatz und klassifiziert KI-Systeme anhand ihrer Risiken in Systeme mit inakzeptablem, hohem, begrenztem und minimalem Risiko, für welche jeweils unterschiedliche Vorschriften gelten.¹¹³ Sie nimmt die Gesichtserkennungstechnologie zu Strafverfolgungszwecken besonders ins Visier: «Biometrische Echtzeit-Fernidentifizierungssysteme» werden als KI-Systeme mit inakzeptablem Risiko eingestuft und deren Verwendung in öffentlich zugänglichen Räumen zu Strafverfolgungszwecken wird verboten (Art. 5 lit. d KI-Verordnung). Das Verbot der Echtzeit-Gesichtserkennung wird zwar durch eine weitreichende Ausnahmeregelung relativiert,¹¹⁴ diese Ausnahmen werden allerdings ihrerseits strikten Voraussetzungen unterstellt und erfordern neben einer Interessenabwägung eine Genehmigung einer Justiz- oder unabhängigen Verwaltungsbehörde (Art. 5 Abs. 2 und 3 KI-Verordnung). Ein solches Teilverbot von Echtzeit-Gesichtserkennungssystemen wäre in der Schweiz eigentlich nicht notwendig.¹¹⁵ Ohne formell-gesetzliche Grundlagen sind Einsätze von Echtzeit-Gesichtserkennungssystemen nicht zulässig und deshalb ohnehin verboten.

Die KI-Verordnung nimmt auch nachträgliche Gesichtserkennungssysteme ins Visier. KI-Systeme zur nachträglichen biometrischen Fernidentifizierung gelten als «Hochrisiko-KI-Systeme» (Art. 6 Abs. 2 i. V.m. Anhang III Nr. 1 KI-Verordnung). Sie sind grundsätzlich zugelassen, müssen aber den in Kap. 2 der KI-Verordnung festgelegten Anforderungen genügen. Diese Anforderungen

112 Dazu schon NADJA BRAUN BINDER et al., Künstliche Intelligenz: Handlungsbedarf im Schweizer Recht, Jusletter vom 28.06.2021, N 16 ff.

113 ANGELA MÜLLER, Der Artificial Intelligence Act der EU: Ein risikobasierter Ansatz zur Regulierung von Künstlicher Intelligenz – mit Auswirkungen auf die Schweiz, Zeitschrift für Europarecht 2022, A 6 ff.

114 Die Verwendung wird erlaubt, wenn dies unbedingt erforderlich ist für i) die Suche nach potenziellen Opfern von Straftaten, ii) die Abwendung unmittelbar drohenden Gefahren oder iii) zur Erkennung, Aufspürung, Identifikation oder Verfolgung von straffälligen oder verdächtigen Personen, sofern die Tat mit freiheitsentziehenden Massnahmen von mind. drei Jahren bedroht ist.

115 BRAUN BINDER/KUNZ/OBRECHT (Fn. 5), N 61.

umfassen bspw. die Einrichtung eines Risikomanagementsystems, Vorgaben hinsichtlich Datensätze und Trainingsdaten, Transparenzpflichten, die Möglichkeit zur menschlichen Aufsicht und ein angemessenes Mass an Genauigkeit des Systems.¹¹⁶ Nachträgliche Gesichtserkennungssysteme müssen als Hochrisiko-KI-Systeme somit eine breite Palette an Anforderungen erfüllen.¹¹⁷ Automatisierte Gesichtserkennung, wie sie bis anhin in der Schweiz zum Einsatz kommt, wäre im EU-Recht also ein Hochrisiko-KI-System. In den EU-Mitgliedstaaten ist deren konkrete rechtliche Zulässigkeit – in Einklang mit der KI-Verordnung – im nationalen Strafprozessrecht vorzusehen. Die Verordnung liefert keine eigenständige Grundlage zur Rechtfertigung entsprechender Grundrechtseingriffe.

II. Ansprüche an eine strafprozessrechtliche Regelung

Das schweizerische Strafprozessrecht enthält *de lege lata* keine Rechtsgrundlage für Einsätze automatisierter Gesichtserkennung. Das gilt für Echtzeit-Gesichtserkennungssysteme wie für nachträglich eingesetzte Software. Soll das geändert werden, müsste der Gesetzgeber eigens dafür vorgesehene Normen schaffen. Die Regelung hätte den Datenbearbeitungsprozess mit Blick auf die jüngste Rechtsprechung in hoher Bestimmtheit zu regeln. Die mit der automatisierten Gesichtserkennung einhergehende qualifizierte Form der Datenanalyse wäre deshalb als eigenständige Zwangsmassnahme im 5. Titel der StPO vorzusehen.

In der StPO festgehalten werden müssten die Voraussetzungen der mit der Gesichtserkennung verbundenen Grundrechtseingriffe, d.h. der gesamte Datenbearbeitungsprozess. Einerseits müsste gesetzlich vorgesehen werden, dass Gesichtsbilder mit einem spezifischen technischen Verfahren biometrisch erfasst werden dürfen (Erstellung biometrischer Daten). Andererseits müsste normiert werden, dass die biometrisch erfassten Gesichtsbilder mit weiteren bereits erfassten Gesichtsbilddaten abgeglichen werden dürfen (Abgleich biometrischer Daten). Hierfür müsste geregelt werden, welche Gesichtsbilddaten zum Abgleich herangezogen werden dürfen, inklusive einer Eingrenzung, mit welchen Datenbanken Datenabgleiche durchgeführt werden dürfen.

Soll die automatisierte Gesichtserkennung erlaubt werden, wäre festzulegen, in welchen Fällen diese zum Einsatz kommen darf. So wäre bspw. die Verankerung eines Kataloges von schweren Straftaten denkbar (wie z.B. in Art. 269 Abs. 2 oder Art. 286 Abs. 2 StPO). Vorzusehen wären auch die Kompetenzen zur Anordnung und das Anordnungsverfahren selbst, z.B. im Sinne eines Schriftlichkeitserfordernisses. Es wäre zudem regulatorisch angezeigt, flankierende Massnahmen zur Vermeidung negativer Auswirkungen auf Grund- und

116 MARTINI (Fn. 25), S. 16.

117 MARTINI (Fn. 25), S. 16.

Freiheitsrechte vorzusehen. Technische, organisatorische und verfahrensrechtliche Anforderungen sollten in einem Spezialgesetz im Sinne von Mindestanforderungen normiert werden. Dazu würde sicherlich das Erfordernis von Transparenz und die Nachvollziehbarkeit der Systeme gehören. Die Ergebnisse müssen verifizierbar sein. Gleichzeitig müssten die Systeme ein angemessenes Mass an Genauigkeit aufweisen. Vor einer Verwendung ist sicherzustellen, dass die Systeme bzw. deren Datensätze keine diskriminierenden Verzerrungen aufweisen. Hinsichtlich dieser Anforderungen könnte man sich sicherlich massgeblich an die KI-Verordnung der EU anlehnen.

Schliesslich wäre bei einer beschränkten Erlaubnisnorm der Rechtsschutz zu bedenken. Eine vom Gesichtserkennungssystem identifizierte Person muss die Möglichkeit haben, die Richtigkeit der Identifikation überprüfen zu lassen, da das Risiko besteht, aufgrund einer dem System immanenten Fehlerquote zu Unrecht in Verdacht zu geraten.¹¹⁸ In Anbetracht der freien Beweiswürdigung stellen sich hier ungelöste Herausforderungen mit dem Umgang statistischer Wahrscheinlichkeiten von KI-Systemen. Derartige Fragen sind heute noch unzureichend geklärt, müssten aber vor einem Einsatz von KI im Strafverfahren debattiert werden. Um eine verfassungskonforme Anwendung zu gewährleisten, könnte zusätzlich eine Kontrolle durch eine unabhängige Stelle vorgesehen werden. Auf diese Weise kann sichergestellt werden, dass die automatisierten Datenbearbeitungen – wie vom Bundesgericht im Zusammenhang mit der AFV ausdrücklich gefordert – nicht zu Überwachungszwecken missbraucht und die gesetzlichen Anforderungen eingehalten werden.¹¹⁹

G. Fazit

Wenn so lange und kreativ nach Rechtsgrundlagen für eine Ermittlungsmassnahme gesucht werden muss, ist die Antwort zu deren Rechtmässigkeit schon gefunden. Gäbe es ausreichend bestimmte Rechtsgrundlagen für die automatisierte Gesichtserkennung, wären diese einfach zu benennen, was offenkundig nicht der Fall ist. Sie bleibt also unrechtmässig. In der Auseinandersetzung mit biometrischen Analyseverfahren und der rechtlichen Erfassung solcher digitaler Ermittlungsmassnahmen offenbaren sich allerdings legistische Herausforderungen genereller Natur. Es zeigt sich zudem deutlich, dass wir rechtswissenschaftlich und gesellschaftspolitisch zu diskutieren haben, wie wir mit solchen Methoden strafprozessual umgehen wollen und wie wir die StPO «fit» für das digitale Zeitalter machen. Die Ermittlungsarbeit ist zunehmend digital. Dem hat auch die StPO Rechnung zu tragen.

118 BGer 1C_39/2021 v. 29.11.2022, E. 8.1.1.

119 Siehe dazu die Vorgaben in BGer 1C_39/2021 v. 29.11.2022, E. 8.11.2.

Angesichts der rasanten technologischen Entwicklung einerseits und dem schwerfälligen Gesetzgebungsverfahren andererseits, scheint es für die Strafverfolgungsbehörden eine verlockende Option zu sein, an die Bestimmtheit von Rechtsgrundlagen zugunsten der Strafverfolgung geringe Massstäbe zu setzen.¹²⁰ Dies ist nicht opportun. Die Anforderungen an den Grundrechtsschutz sind im digitalen Zeitalter hochzuhalten. Moderne Technologien haben gerade im Überwachungsbereich das Potenzial, unsere Freiheitsrechte auf ganz wesentliche Weise zu beschränken. Es sollte diskutiert werden, wie «technologieneutrale» Normen geschaffen werden können, welche die Rahmenbedingungen des Technikeinsatzes deutlich vorgeben, sogleich aber nicht nur einzelne Technologien fokussieren, um mit der Entwicklung Schritt halten zu können. Die Antwort auf den technischen Fortschritt wären solch technologieneutrale Leitplanken mit klar definierten roten Linien, nicht Abstriche beim Rechtsstaat. Abstriche bei den rechtlichen Grundlagen sind deshalb nicht angezeigt. Die Bevölkerung muss voraussehen können, was für Eingriffe in ihre Rechte unter welchen Voraussetzungen drohen. Solche Eingriffe sind zudem demokratisch zu legitimieren. Es ist am Gesetzgeber zu entscheiden, welche Ermittlungsinstrumente der Polizei zur Verfügung stehen sollen.

Zusammenfassung

Die automatisierte Gesichtserkennung etabliert sich als Ermittlungsmassnahme im Strafverfahren, obwohl deren Rechtmässigkeit umstritten ist. Die Autorinnen haben dazu in einer Publikation vor knapp zwei Jahren Stellung bezogen und dargelegt, weshalb für den Einsatz automatisierter Gesichtserkennung keine ausreichenden Rechtsgrundlagen bestehen. In der Zwischenzeit hat sich der Diskurs über die Zulässigkeit der Nutzung von Gesichtserkennungstechnologie im Strafverfahren intensiviert. Dieser Beitrag knüpft an diese bisherige Debatte an und unterzieht die von verschiedener Seite zur Rechtfertigung des Einsatzes hervorgebrachten Rechtsgrundlagen einer Prüfung. Die Auseinandersetzung bestätigt, dass *de lege lata* keine ausreichenden gesetzlichen Grundlagen für den Einsatz automatisierter Gesichtserkennung im Strafverfahren bestehen. In Anlehnung an die KI-Verordnung der EU diskutiert der Beitrag deshalb, wie eine strafprozessrechtliche Regulierung der Gesichtserkennung *de lege ferenda* aussehen könnte. Für automatisierte biometrische Analyseverfahren sind Normen zu schaffen, welche die mit ihnen einhergehenden schweren Grundrechtseingriffe in ihrer Gesamtheit abbilden. Dazu gehört nicht nur die Beschaffung von Daten durch den Staat, sondern auch deren Analyse und Verwertung.

120 So explizit vorgeschlagen von KÜHNE (Fn. 2), S. 13 und 24.

Résumé

La reconnaissance faciale automatique s'établit peu à peu comme mesure d'investigation au sein de la procédure pénale, bien que sa légalité soit controversée. Il y a près de deux ans, les autrices avaient pris position sur la question et démontré que les bases légales n'étaient pas suffisantes pour justifier l'utilisation de la reconnaissance faciale dans la procédure pénale. Entre-temps, le débat autour de l'admissibilité de l'utilisation de ces technologies au sein de la procédure pénale s'est intensifié. Cette contribution s'inscrit dans le prolongement de ce débat en analysant les bases légales proposées par différentes parties pour justifier l'utilisation de la reconnaissance faciale automatique dans la procédure pénale. L'analyse *de lege lata* confirme qu'il n'existe pas de bases légales suffisantes pour justifier l'utilisation de ces technologies. En prenant appui sur l'AI Act de l'Union Européenne, une réglementation *de lege ferenda* de la reconnaissance faciale au sein de la procédure pénale est discutée. Il faut créer des normes qui reflètent dans leur ensemble les graves atteintes aux droits fondamentaux qu'ils impliquent. Cela ne concerne pas seulement la collecte des données, mais aussi leur analyse et exploitation.