RISIKO

POLIZEI & MILITÄR

Anstieg der Kriminalität in der Schweiz: Zur Bedeutung des Faktors Staatsangehörigkeit
[Dirk Baier]

TECHNIK & INFRA-STRUKTUR

Automatisierte Informationsverarbeitung im Strafverfahren: Hinreichende Zweckbestimmung als Gradmesser der Verhältnismässigkeit
[Elena Biaggini]

RISIKO & RECHT AUSGABE 02 / 2024

RECHT

Automatisierte Informationsverarbeitung im Strafverfahren: Hinreichende Zweckbestimmung als Gradmesser der Verhältnismässigkeit

Elena Biaggini*

Der zunehmende Einsatz von automatisierten Informationsverarbeitungsmethoden zum Zwecke der Strafverfolgung verlangt nach hinreichend bestimmten rechtlichen Rahmenbedingungen, an welchen es de lege lata noch fehlt. Vor dem Hintergrund der mannigfachen Nutzungs- und Kombinationsmöglichkeiten bildet eine hinreichende Zweckbestimmung sowie Zweckbindung dieser Informationen den Gradmesser der Verhältnismässigkeit solcher Massnahmen. Eine Verhältnismässigkeitsprüfung im Einzelfall bleibt nach wie vor unentbehrlich.

Inhalt

* Dr. iur. Elena Biaggini, LL.M., ist Substitutin bei Umbricht Rechtsanwälte AG (Zürich). Zuvor hat sie am Lehrstuhl für Strafrecht und Strafprozessrecht an der Universität Zürich bei Prof. Dr. iur. Sarah Summers promoviert. Anm. der Herausgeberschaft: Die Dissertation der Autorin „Verwertbarkeit verdachtsbegründender Informationen aus Fernmeldeüberwachungen im Strafverfahren. Vorschlag eines Verwertbarkeitskonzepts für Informationen aus der präventiven und repressiven Überwachung des Fernmeldeverkehrs auf strafprozessualer und verfassungsrechtlicher Grundlage“ erschien im Jahre 2022; sie wurde mit dem Professor Walther Hug-Preis für Dissertationen ausgezeichnet.

I. Einleitung

Die Beweisführung im Strafverfahren ist von einem Strukturwandel geprägt. Im Zuge des technologischen Fortschritts gewinnen neben tradierten Formen der Beweiserhebung zunehmend auch neue Formen der Informationsbeschaffung zu Ermittlungszwecken sowie zwecks Beweisführung im Strafverfahren an Bedeutung. Automatisiert stattfindende Informationserhebungs- und Verarbeitungsmethoden wie etwa der Einsatz von Antennensuchläufen im Rahmen einer Rasterfahndung, der automatisierten Fahrzeugfahndung und Verkehrsüberwachung (AFV) und Gesichtserkennungstechnologien ermöglichen neue Formen der Informationsbeschaffung, die sich zunehmend von der punktuellen Beweiserhebung entfernen.[1] Solche neuen Formen der Informationsbeschaffung zeichnen sich aufgrund ihrer Streubreite und der mannigfachen Nutzungsmöglichkeiten ausserhalb ihres ursprünglichen Erhebungszwecks durch eine besondere Eingriffsintensität aus und erfordern daher klare rechtliche Rahmenbedingungen.

[1] Dazu bereits BIAGGINI, Rz. 16 und Rz. 23.

Insbesondere in jüngster Zeit hat sich der Diskurs um den Einsatz automatisierter Informationsverarbeitungsvorgänge wie namentlich Gesichtserkennungstechnologien im Polizei- und Strafprozessrecht im Schrifttum intensiviert.[2] Auch die Rechtsprechung befasst sich zunehmend mit der Rechtmässigkeit des Einsatzes automatisierter Informationsverarbeitungsvorgänge zu Ermittlungs- und Fahndungszwecken sowie der Verwertbarkeit der hieraus erlangten Informationen im Strafverfahren.[3] Dabei wird die Debatte bislang in erster Linie punktuell im Hinblick auf konkrete automatisierte Informationsbeschaffungsmassnahmen geführt, wobei die Zulässigkeit der jeweiligen Massnahme nach dem heutigen Gesetzesstand im Vordergrund steht.[4]

Die fortwährende Debatte wirft ein Licht auf die grundlegende Problematik, dass die in Form von Zwangsmassnahmen gekleideten strafprozessualen Vorschriften der Informationsbeschaffung in erster Linie auf die punktuelle Informationserhebung zu Beweiszwecken und nicht auf die mit dem technologischen Fortschritt einhergehenden neuen Formen der maschinellen Informationsverarbeitung zugeschnitten sind.

Gegenstand der vorliegenden Untersuchung bildet die Fragestellung, welche konkreten (verfassungs-)rechtlichen Anforderungen sich an die Ausgestaltung von Gesetzesgrundlagen für die automatisierte Informationsverarbeitung zu Strafverfolgungszwecken stellen. Aufgrund der Ähnlichkeit der sich jeweils aufdrängenden Fragestellungen erscheint es dabei sachgerecht, die verschiedenen derzeit diskutierten automatisierten Informationsbeschaffungsmassnahmen einander gegenüberzustellen (II.) und anhand dessen einige allgemeingültige Leitlinien zu erarbeiten (V.). Dabei weisen die Vorgaben des grundrechtlichen Datenschutzes (III.) sowie die im Zusammenhang mit der automatisierten Fahrzeugfahndung und Verkehrsüberwachung (AFV) ergangene bundesgerichtliche Rechtsprechung[5] (IV.1) klar in die Richtung, dass aufgrund der Eingriffsintensität solcher Massnahmen strenge Anforderungen an die hinreichende gesetzliche Grundlage zu stellen sind.

---

2 SIMMLER/CANOVA, Gesichtserkennung, 201 ff.; SIMMLER/CANOVA, „Smarte" Polizeiarbeit, 105 ff.; KÜHNE, 13 ff. Zur Zulässigkeit der maschinellen Gesichtserkennung im öffentlichen Raum BRAUN BINDER/KUNZ/OBRECHT, 53 ff.

3 Vgl. BGE 137 IV 340 (Antennensuchlauf) sowie BGE 146 I 11 und BGE 149 I 218 (AFV).

4 Vgl. dazu SIMMLER/CANOVA, Gesichtserkennung, 212 ff.; KÜHNE, 20 ff. Unbestritten ist, dass keine kantonalen polizeirechtlichen Grundlagen bestehen, SIMMLER/CANOVA, „Smarte" Polizeiarbeit, 116; BRAUN BINDER/KUNZ/OBRECHT, Rz. 29; KÜHNE, 19.

5 BGE 149 I 218; BGE 146 I 11.

II. Automatisierte Informationsbeschaffungsmethoden als neue Formen der Beweisbeschaffung

Die automatisierte Bearbeitung von Personendaten i.S.v. Art. 5 lit. a DSG, vorliegend verstanden als die zumindest teilweise maschinell und ohne menschliches Zutun[6] erfolgende Erhebung, Abgleichung und Auswertung von Personendaten, stellen in verschiedener Hinsicht gewissermassen eine qualifizierte Form der Informationsbeschaffung zu Ermittlungszwecken dar. So ermöglichen automatisierte Informationsverarbeitungssysteme eine systematische Erfassung und simultane Bearbeitung grosser Datenmengen innert Sekundenbruchteilen, was sie von herkömmlichen manuellen Auswertungsmöglichkeiten wesentlich unterscheidet.[7] Kennzeichnend für diese neuen Formen der Informationsbeschaffung ist weiter, dass hierbei nicht bloss Beweise im klassischen Sinn erhoben werden, sondern durch die Bearbeitungsvorgänge und den (automatisierten) Abgleich dieser Daten mit anderen Datensammlungen neue Informationen generiert,[8] beliebig neu kombiniert sowie auch potenziell in beliebigem anderem Sachzusammenhang verwendet werden können.[9] Dies lässt selbst die Erfassung an sich belangloser Daten in einem neuen Licht erscheinen.[10]

Das Nutzungspotential solcher umfassenden Datenerhebungen reicht von der Überprüfung eines konkreten Tatverdachts bis zur Verwendung solcher Informationen im Rahmen von Strukturermittlungen.[11] Damit stehen solche neuen Informationsverarbeitungsvorgänge evidentermassen in einem latenten Spannungsverhältnis zum Grundsatz der verdachtsgesteuerten Beweisführung im

---

6 Auch im Rahmen der automatisierten Datenbearbeitung ist nicht vorausgesetzt, dass die Bearbeitung vollautomatisiert und damit gänzlich ohne menschliches Zutun erfolgt, vgl. EJPD, Totalrevision des Datenschutzgesetzes: Häufig gestellte Fragen, Februar 2024, 8, abrufbar unter <https://www.ejpd.admin.ch/bj/de/home/staat/datenschutz/faq.html>. Namentlich die Auswertung des Schnittmengenergebnisses erfolgt in der Regel manuell, vgl. für den Antennensuchlauf Biaggini, Rz. 175; für die automatisierte Gesichtserkennung etwa Kühne, 15.

7 Vgl. für die AFV BGE 146 I 11 E. 3.2. Auf diese Problematik ebenso hinweisend Simmler/Canova, Gesichtserkennung, 211.

8 Vgl. zur Unterscheidung zwischen Daten und Informationen, wobei letztere Sinngehalte darstellen, die sich aus der Interpretation von Daten ergeben Albers, 89 ff.; Biaggini, Rz. 364 f.

9 Für die AFV BGE 146 I 11 E. 3.2.

10 Vgl. dazu BVerfGE 120, 378 (398 f.), wonach es mit der Möglichkeit der automatischen Datenverarbeitung keine „belanglosen Daten" mehr gebe.

11 Vgl. Gless, 171; Biaggini, Rz. 116.

Strafverfahren.[12] Vor diesem Hintergrund bedürfen neben der Rechtmässigkeit der Erhebung auch die Zulässigkeit und Schranken der weiteren Verwendung der einmal erhobenen Informationen einer näheren Betrachtung.

Zugleich ist automatisierten Informationsbeschaffungsmethoden gemeinsam, dass sie sich, anders als tradierte strafprozessuale Zwangsmassnahmen, regelmässig nicht nur gegen eine bestimmte (in der Regel die tatverdächtige) Person richten, sondern aufgrund ihrer Streubreite potenziell eine Vielzahl von Personen tangieren, die keinen Anlass für die Überwachung gegeben haben.[13] Dabei ist auch auf die potenziell nicht unerhebliche Fehlerquote hinzuweisen, die mit solchen automatisierten Informationsverarbeitungsmethoden einhergehen kann.[14] So besteht die latente Gefahr, dass Betroffene zu Unrecht unter Verdacht geraten.[15] Ein zurückhaltender Einsatz von automatisierten Informationsverarbeitungsvorgängen zu Strafverfolgungszwecken[16] gebietet sich auch deshalb, weil der Eingriff in die Rechtspositionen unbeteiligter Dritter bereits vorab feststeht.[17]

Bereits heute kommen automatisierte Informationsverarbeitungsvorgänge zu Ermittlungszwecken im Strafverfahren zum Einsatz.[18] Das Bedürfnis, automatisierte Informationsverarbeitungstechnologien künftig vermehrt einzusetzen, dürfte zudem in Anbetracht der insbesondere in jüngerer Zeit verstärkt in den Fokus gerückten Problematik der Überlastung der Justiz weiter zunehmen.

Nachfolgend soll die Funktionsweise automatisierter Informationsbeschaffungsmethoden anhand dreier Beispiele skizziert werden. Vorweggenommen sei, dass diese zu erheblichen Grundrechtseingriffen[19] führen und daher

---

12 Vgl. dazu bereits Biaggini, Rz. 171.

13 Vgl. BGE 149 I 218 E. 8.2.3.

14 Vgl. im Zusammenhang mit der AFV BGE 146 I 11 E. 3.2.

15 Vgl. im Zusammenhang mit der AFV BGE 146 I 11 E. 3.2; siehe auch BGE 124 I 80 E. 2e; Simmler/Canova, Gesichtserkennung, 224.

16 So beispielsweise die Beschränkung auf einen Deliktskatalog bzw. den Ausschluss von Bagatellfällen und leichten Delikten.

17 Siehe für den Antennensuchlauf Biaggini, Rz. 171; für die DNA-Massenuntersuchung BSK StPO-Fricker/Maeder, Art. 256 N 9.

18 So werden etwa im Kanton St. Gallen bereits Gesichtserkennungstechnologien zu Ermittlungszwecken eingesetzt, vgl. dazu Kühne, 15. Für den Einsatz von Antennensuchläufen vgl. den Leitentscheid BGE 137 IV 340 sowie den medial bekannt gewordenen Fall „Ruppers-wil", dazu Forster, 357 f. Zur Verwendung von Informationen aus der AFV im Strafverfahren BGE 146 I 11.

19 So insbesondere das Recht auf informationelle Selbstbestimmung nach Art. 13 Abs. 2 BV, vgl. hierzu nachfolgend unter Kap. III.

rechtliche Rahmenbedingungen fordern. Zugleich illustriert die Gegenüberstellung, dass die verschiedenen Massnahmen, wenngleich sie in unterschiedlichen Einsatzbereichen zur Anwendung gelangen, einige gemeinsame Grundzüge aufweisen. Dies weist in die Richtung, das Augenmerk bei der Beurteilung der Zulassung solcher automatisierten Informationsverarbeitungssysteme neben massnahmenspezifischen Vorgaben auch auf gewisse allgemeingültige Leitplanken zu legen.

1. Antennensuchlauf im Rahmen einer Rasterfahndung

Der Antennensuchlauf im Rahmen einer Rasterfahndung dient als Ermittlungsmassnahme zur Eruierung der noch unbekannten Täterschaft bei Vorliegen eines tatbezogenen Verdachts.[20] So lässt sich rückwirkend anhand von Mobiltelefon-Randdaten etwa eruieren, welche Personen sich im Tatzeitraum im Bereich des mutmasslichen Tatortes aufgehalten haben.[21] Dabei werden in einem ersten Schritt rückwirkend sämtliche Randdaten während eines bestimmten Zeitraums an einem bestimmten Mobilfunkantennenstandort – etwa dem mutmasslichen Tatort – erhoben.[22] Die zunächst anonymisiert erhobenen Datensätze können daraufhin durch die Untersuchungsbehörden mit den Randdaten von anderen Standorten abgeglichen respektive anhand weiterer festgelegter ermittlungsrelevanter Parameter ausgewertet werden,[23] um die mutmassliche Täterschaft auf einen möglichst kleinen Kreis an Personen zu beschränken bzw. diese zu identifizieren.[24]

Damit lassen sich beim Antennensuchlauf grob drei potenziell grundrechtlich relevante Bearbeitungsschritte ausmachen:[25] *Erstens* das Erheben sämtlicher Randdaten an den festgelegten Antennenstandorten; *zweitens* der Datenabgleich der erfassten Randdaten zur Bildung einer Schnittmenge und deren Abgleich mit den übrigen Untersuchungsergebnissen im Rahmen einer Rasterfahndung; sowie *drittens* die Identifikation der in das Fahndungsraster fallenden Personen und die weitere Nutzung dieser Informationen im Verfahren.

---

20 Vgl. zu Begrifflichkeit und Funktionsweise etwa Forster, 358; Hansjakob, Überwachungsrecht, Rz. 862; ZK StPO-Hansjakob/Pajarola, Art. 273 N 20; Roos/Jeker, 176 f.

21 So etwa der dem Entscheid BGE 137 IV 340 zugrundeliegende Sachverhalt.

22 Siehe dazu im Einzelnen Biaggini, Rz. 174 ff.; vgl. auch BGE 137 IV 340 E. 5.4.

23 Vgl. Hansjakob, Überwachungsrecht, Rz. 874; vgl. auch BGE 137 IV 340 E. 6.6; Forster, 358.

24 Vgl. BGE 137 IV 340 E. 5.6 sowie E. 6.5.

25 Vgl. dazu bereits Biaggini, Rz. 182.

2. Automatisierte Fahrzeugfahndung und Verkehrsüberwachung

Bei der automatisierten Fahrzeugfahndung und Verkehrsüberwachung (AFV) werden die Kontrollschilder von vorbeifahrenden Fahrzeugen anhand mobiler oder stationärer Kameraräte erfasst und ein Datensatz mit den Buchstaben und Ziffern des Kontrollschilds zwecks Abgleich mit anderen Datenbanken erzeugt.[26] Je nach Modalitäten der Datenauswertung werden neben der Identität des Fahrzeughalters auch der Zeitpunkt der Kontrolle, der Standort, die Fahrtrichtung sowie weitere Fahrzeuginsassen erfasst.[27] Entsprechend können AFV-Abfragen sowohl zu Ermittlungs- als auch zu Fahndungszwecken eingesetzt werden. So betreibt etwa das Bundesamt für Zoll und Grenzsicherheit (BAZG) AFV-Systeme zwecks automatischer Kontrollschilderkennung zur Bekämpfung grenzüberschreitender Kriminalität.[28] Zudem wurde die Einführung entsprechender Bestimmungen in kantonalen Polizeigesetzen bereits bundesgerichtlich beurteilt.[29]

Anders als beim Antennensuchlauf, welcher im Nachgang einer Straftat angeordnet wird, ist zumindest das Erfassen von Fahrzeugkontrollschildern mittels AFV an sich der präventiv-polizeilichen Kontrolltätigkeit zuzuordnen, welche dem kantonalen Recht unterliegt.[30] Dies zeigt sich auch daran, dass die Messstationen verdachtsunabhängig zum Einsatz gelangen und zunächst anlasslos jedes vorbeifahrende Fahrzeug erfassen. Indessen ist der Übergang in die kriminalpolizeiliche Tätigkeit hier fliessend. Sobald die Informationen im Rahmen strafprozessualer Ermittlungen verwendet werden sollen, wird der Anwendungsbereich der StPO eröffnet und die Ermittlungshandlungen der Polizei fallen unter die Vorschriften gemäss Art. 306 ff. StPO.[31]

3. Automatisierte Gesichtserkennung

Bei der maschinellen Gesichtserkennung werden anhand von digitalen Bildern Gesichtsmerkmale natürlicher Personen automatisch zu maschinenlesbaren Templates zwecks Identifizierung, Authentifizierung bzw. Verifizierung oder

---

26 BGE 149 I 218 E. 8.1.1 sowie Urteil des Bundesgerichts 6B_908/2018 vom 7. Oktober 2019 E. 2.1 (nicht publ. in BGE 146 I 11).

27 Vgl. BGE 146 I 11 E. 3.2; BGE 149 I 218 E. 8.1.1.

28 Vgl. dazu Interpellation Pointet 23.3507.

29 BGE 146 I 11 (Kanton Thurgau); BGE 149 I 218 (Kanton Solothurn).

30 Vgl. BGE 146 I 11 E. 4.1.

31 BGE 146 I 11 E. 4.1.

Kategorisierung verarbeitet.[32] Regelmässig knüpfen Gesichtserkennungstechnologien dabei an Videoüberwachungssysteme des öffentlichen Raums an.[33] In Zusammenhang mit Strafverfolgungszwecken lässt sich etwa anhand von Gesichtserkennungstechnologien Bildmaterial eines mutmasslichen Täters auf einer Überwachungskamera im Nachgang einer Straftat auswerten und mit Bildmaterial etwa aus Polizeidatenbanken abgleichen.[34] Umgekehrt lässt sich Videomaterial etwa von Überwachungskameras aber auch dahingehend auswerten, ob darauf eine konkrete Person zu erkennen ist.[35] Die Datenverarbeitung betrifft damit nicht eine einzelnen konkreten Zielperson, sondern greift unweigerlich in die Rechtsposition sämtlicher Personen ein, deren Gesichter zwecks eines Abgleiches erfasst und bearbeitet werden.[36] Die automatisierte Gesichtserkennung stellt in der vorliegenden Gegenüberstellung die vergleichsweise eingriffsintensivste Massnahme dar, denn es werden hierbei in einem (Masse-)Analyseverfahren biometrische Daten[37] i.S.v. Art. 5 lit. c Ziff. 4 DSG bearbeitet, die das Gesetz als besonders schützenswert qualifiziert.[38]

Auch bei Gesichtserkennungstechnologien reicht der Einsatzbereich von der dem präventiv-polizeilichen Bereich zuzuordnenden allgemeinen (anlasslosen) Überwachung des öffentlichen Raums zu Sicherheitszwecken[39] und sicherheitspolizeilichen Massnahmen der konkreten Gefahrenabwehr etwa an Grossveranstaltungen bis zum repressiven Einsatz der automatischen Gesichtserkennung zu Ermittlungs- und damit zu Strafverfolgungszwecken.[40] Diese Unterscheidung ist deshalb von Bedeutung, weil sich präventive und re-

---

32 Vgl. Braun Binder/Kunz/Obrecht, Rz. 5; Simmler/Canova, Gesichtserkennung, 207.

33 Siehe Simmler/Canova, „Smarte" Polizeiarbeit, 110.

34 Vgl. Braun Binder/Kunz/Obrecht, Rz. 14; Simmler/Canova, „Smarte" Polizeiarbeit, 105 f.

35 Vgl. zum Ganzen Simmler/Canova, Gesichtserkennung, 204.

36 Siehe auch Simmler/Canova, Gesichtserkennung, 208.

37 Gemäss Art. 5 lit. c Ziff. 4 DSG sind dies Daten, die eine natürliche Person eindeutig identifizieren; vgl. Botschaft des Bundesrates vom 15. September 2017 zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBl 2017, 6941 ff., 7020.

38 Siehe ebenso Simmler/Canova, Gesichtserkennung, 207, 211 m.w.H. zur KI-Verordnung der EU.

39 Etwa indem man bestehende Videoüberwachungsinfrastruktur im öffentlichen Raum durch Gesichtserkennungstechnologien ergänzt, siehe dazu Simmler/Canova, „Smarte" Polizeiarbeit, 109.

40 Siehe dazu Simmler/Canova, Gesichtserkennung, 205 f.; Simmler/Canova, „Smarte" Polizeiarbeit, 109 f.

pressive Zweckausrichtungen grundlegend unterscheiden und von der Zulässigkeit des einen nicht ohne Weiteres auf die Zulässigkeit des anderen Verwendungszwecks geschlossen werden darf.[41]

Wiederum finden mit der Erhebung der Ausgangsdaten, dem Abgleich der Daten mit Vergleichsdatenbanken und der weiteren Verwendung der hieraus resultierenden Datentreffer mehrere Bearbeitungsschritte statt, welche jeweils für sich genommen in die Grundrechtspositionen der betroffenen Personen eingreifen.[42]

III. Vorgaben an automatisierte Informationsverarbeitungsvorgänge aus dem verfassungsrechtlichen Datenschutz

Automatisierte Informationsverarbeitungsvorgänge sind aus verfassungsrechtlicher Sicht jedenfalls nicht ohne Weiteres zum Zwecke der Beweisführung im Strafverfahren zulässig. Denn die vorgenannten Informationsverarbeitungsvorgänge führen zu Eingriffen in das Recht auf Privatsphäre nach Art. 13 Abs. 1 BV wie auch in das in Art. 13 Abs. 2 BV verankerte Recht auf informationelle Selbstbestimmung[43] bzw. in den grundrechtlichen Anspruch auf Datenschutz. Damit sind automatisierte Informationsverarbeitungsvorgänge zu Ermittlungszwecken sowie zwecks Beweissicherung aus strafprozessualer Sicht als Zwangsmassnahmen im Sinne von Art. 196 StPO zu qualifizieren.[44] Sie bedürfen entsprechend einer hinreichenden gesetzlichen Grundlage (Art. 197 Abs. 1 StPO). Sollen solche Informationseingriffe im Strafverfahren für zulässig erklärt werden, gilt es, die in Art. 13 Abs. 2 BV enthaltenen verfassungsrechtlichen Determinanten zu beachten. Vorwegzunehmen sei, dass sich aus dem verfassungsrechtlichen Datenschutz und dem hierin enthaltenen Grundsatz der Zweckbindung namentlich gesteigerte Anforderungen an den Bestimmtheitsgrad der Norm in Bezug auf die zulässigen Verarbeitungsvorgänge sowie an die Verhältnismässigkeit der Informationsverarbeitung ergeben.

---

41 Zum Grundsatz der Zweckbindung als Teilgehalt des verfassungsrechtlichen Datenschutzes siehe nachfolgend Kap. III.2.

42 Vgl. dazu nachfolgend Kap. III.; zum Ganzen auch Simmler/Canova, „Smarte" Polizeiarbeit, 112.

43 Vgl. hierzu G. Biaggini, OFK BV, Art. 13 N 11; BSK BV-Diggelmann, Art. 13 N 32.

44 Siehe für den Antennensuchlauf Biaggini, Rz. 181; Roos/Jeker, 179; implizit auch BGE 137 IV 340 E. 6.1; für die automatisierte Gesichtserkennung Simmler/Canova, Gesichtserkennung, 209.

1. Art. 13 Abs. 2 BV als strukturelle Garantie

Der in Art. 13 Abs. 2 BV verankerte verfassungsrechtliche Datenschutz[45] gewährleistet Schutz bei sämtlichen Formen der Verarbeitung[46] von Personendaten.[47] Auch Randdaten fallen unter den Schutzbereich, da sie die Identifizierung der Kommunikationsteilnehmer ermöglichen.[48] Der Schutz greift nicht nur bei der missbräuchlichen, sondern bei jeder Form[49] der Verarbeitung. So kann aus verfassungsrechtlicher Sicht selbst aus einer an sich rechtmässigen Informationserhebung nicht unbesehen auf die spätere Verwendung zu einem anderen als dem Erhebungszweck geschlossen werden. Unerheblich für die Eröffnung des Schutzbereiches ist, wie sensibel die fraglichen Informationen sind.[50] Nach bundesgerichtlicher Rechtsprechung ist bereits in der automatisierten Datenerhebung, d.h. unabhängig von einem Datentreffer, ein Eingriff in Art. 13 Abs. 2 BV zu erblicken.[51] Besonders schwer wiegt der Eingriff bei der Bearbeitung biometrischer Daten, wie sie im Rahmen von automatisierten Gesichtserkennungsmassnahmen erhoben werden.[52]

Richtigerweise ist Art. 13 Abs. 2 BV nicht als Anerkennung eines absoluten individualrechtlichen Schutzrechts aufzufassen, nach welchem das Individualinteresse an der umfassenden Unterbindung staatlicher Informationsbearbeitung im Strafverfahren gegenüber dem öffentlichen Aufklärungsinteresse von Straftaten ausnahmslos Vorrang zukommt.[53] Zur Beurteilung der Grundsatzfrage der Zulässigkeit von automatisierten Informationsverarbeitungsvorgängen losgelöst vom einzelnen Anwendungsfall erscheint es ohnehin treffender, den verfassungsrechtlichen Datenschutz nach Art. 13 Abs. 2 BV über den Abwehranspruch des Individuums gegenüber staatlichen Eingriffen hinaus in

---

45 Dazu im Einzelnen Biaggini, Rz. 359; Rz. 369 ff.

46 Namentlich das Erheben, Sammeln, Speichern, Aufbewahren, Bearbeiten und Weitergeben von Personendaten; siehe G. Biaggini, OFK BV, Art. 13 N 11 m.H. auf BGE 137 I 167 E. 3.2; BGE 128 II 259 E. 3.2; Belser, in: Belser/Epiney/Waldmann, § 6 N 87.

47 Bei Personendaten handelt es sich um „*alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen*" (Art. 5 lit a DSG).

48 Siehe BGE 144 I 126 E. 4.2 (Randdaten); BGE 136 II 508 E. 3.2 ff. (IP-Adressen); vgl. auch Urteil des EGMR vom 24.04.2018, *Benedik v. Slovenia*, no. 62357/14, §§ 108 f.

49 G. Biaggini, OFK BV, Art. 13 N 11; BSK BV-Diggelmann, Art. 13 N 33; SGK BV-Schweizer, Art. 13 N 72; vgl. auch BGE 137 I 167 E. 3.2; BGE 128 II 259 E. 3.2.

50 Siehe statt vieler BGE 146 I 11 E. 3.1.1; BGE 136 I 11 E. 3.1.1.

51 Vgl. BGE 149 218 E. 8.10.2; BGE 146 I 11 E. 3.2.

52 SGK BV-Schweizer, Art. 13 BV N 77; siehe auch Simmler/Canova, Gesichtserkennung, 207 f.

53 Vgl. hierzu bereits Biaggini, Rz. 368 f.; zur Einschränkung von Art. 13 Abs. 2 BV im vorliegenden Zusammenhang Kühne, 15.

erster Linie als *strukturelle Garantie* aufzufassen.[54] So lassen sich aus Art. 13 Abs. 2 BV i.V.m. Art. 35 Abs. 1 BV an den Gesetzgeber gerichtete verfassungsrechtliche Mindestanforderungen zur gesetzgeberischen Ausgestaltung des Verfahrensrechts[55] und damit auch an die Regulierung von Informationsverarbeitungsvorgängen im Strafverfahren ableiten.[56]

2. Grundsatz der Zweckbindung

Vor dem Hintergrund der mannigfachen Nutzungsmöglichkeiten einmal erhobener Daten ist im vorliegenden Zusammenhang insbesondere der in Art. 13 Abs. 2 BV verankerte Grundsatz der Zweckbindung von Interesse.[57] Gemäss Art. 6 Abs. 3 DSG dürfen Personendaten nur zu einem bestimmten und für die betroffene Person erkennbaren Zweck beschafft werden und nur so bearbeitet werden, dass es mit diesem Zweck vereinbar ist. Aus dem Grundsatz der Zweckbindung folgt damit zweierlei:[58] Einerseits bedarf jede Datenerhebung einer präzise umschriebenen *Zweckbestimmung*[59] und damit im Kontext strafprozessualer Ermittlungsmassnahmen einer hinreichend bestimmten gesetzlichen Grundlage. Dies gilt dabei für sämtliche Bearbeitungsschritte, die jeweils ihrerseits einen selbstständigen Eingriff in das Recht auf informationelle Selbstbestimmung darstellen. Andererseits sind die erhobenen Daten – und damit auch die Informationen, die sich als Sinngehalte aus der Interpretation der Daten ergeben[60] – an den vorgängig bestimmten Zweck gebunden.[61] Der Zweckbindungsgrundsatz verschafft somit auch die notwendige Transparenz für die betroffenen Personen hinsichtlich der zulässigen Verarbeitungszwecke der über sie erhobenen Daten.[62]

Der hinreichenden Zweckbindung kommt auch deshalb Bedeutung zu, weil sich die gesetzlich vorgesehenen späteren Verwendungsmöglichkeiten bereits

---

54 Grundlegend dazu GÄCHTER/WERDER, 93; siehe bereits auch GÄCHTER/EGLI, Rz. 52 f.; in diesem Sinne auch ALBERS, 147; vgl. im Einzelnen dazu BIAGGINI, Rz. 369 f.

55 Siehe GÄCHTER/EGLI, Rz. 52; GÄCHTER/WERDER, 93.

56 Vgl. dazu bereits BIAGGINI, Rz. 369.

57 Zum Grundsatz der Zweckbindung als Teilgehalt von Art. 13 Abs. 2 BV vgl. G. BIAGGINI, OFK BV, Art. 13 N 13.

58 Dazu im Einzelnen BIAGGINI, Rz. 360 m.w.H.

59 Vgl. dazu BSK DSG-BÜHLMANN/REINLE, Art. 6 N 108 und N 114; ferner BVerfGE 65, 1 (46).

60 Vgl dazu BIAGGINI, Rz. 365.

61 BSK DSG-BÜHLMANN/REINLE, Art. 6 N 113; siehe auch BERTRAM, 139.

62 Vgl. zum Transparenzgrundsatz BSK DSG-BÜHLMANN/REINLE, Art. 6 N 151 ff.

auf die Beurteilung der Intensität des Erhebungseingriffs auswirken.[63] So wiegt die Eingriffsbelastung des Erhebungseingriffs umso schwerer, je vielseitiger die späteren Verwendungsmöglichkeiten der Informationen ausfallen.[64]

3. Anforderungen bei einer Zweckänderung

Der ursprüngliche Bearbeitungszweck bleibt grundsätzlich auch bei einer Weitergabe von Informationen an Dritte beachtlich.[65] Sollen Daten zu einem anderen als ihrem ursprünglichen Erhebungszweck verwendet werden, ist im Bereich der staatlichen Datenverarbeitung eine hinreichend bestimmte gesetzliche Grundlage erforderlich, welche die Datenbearbeitung im Lichte des neuen Verwendungszwecks gestattet.[66] Dabei fordern schwerwiegende Eingriffe wie etwa das Bearbeiten besonders schützenswerter Personendaten oder die Erstellung von Persönlichkeitsprofilen eine gesetzliche Grundlage im formellen Sinn (Art. 36 Abs. 1 BV).[67] Als weiterer Eingriff in Art. 13 Abs. 2 BV muss auch der neue Verwendungseingriff daneben den Anforderungen von Art. 36 Abs. 2 und 3 BV genügen.

Die Problematik um die zweckändernde Verwendung von Daten akzentuiert sich im vorliegenden Kontext an verschiedener Stelle. Eine aus verfassungsrechtlicher Sicht relevante Zweckänderung liegt zunächst dann vor, wenn Informationen, die nunmehr zu Ermittlungszwecken ausgewertet werden sollen, ursprünglich zum Zwecke der Gefahrenabwehr erhoben wurden. Zu denken ist etwa an die Videoüberwachung des öffentlichen Raums in Echtzeit, wie dies vereinzelt bereits an Flughäfen bei der automatisierten Passkontrolle erfolgt.[68] Eine Verwendung der hierdurch erlangten Informationen zu Strafverfolgungszwecken führt zu einer Zweckänderung, welche ihrerseits einer hinreichenden gesetzlichen Grundlage bedarf. Eine Zweckänderung liegt überdies vor, wenn das Ergebnis der Datenauswertung später in einem anderen Sachzusammenhang wie etwa einem anderen Strafverfahren verwendet werden soll. Eine hier nicht näher diskutierte Zweckänderungsproblematik kann sich ferner auch dann stellen, wenn die Datensammlung, mit welcher die Daten abge-

63 Bertram, 140 m.H. auf die deutsche Rechtsprechung.

64 Ebenso Bertram, 140.

65 BSK DSG-Bühlmann/Reinle, Art. 6 N 118.

66 Vgl. Epiney, in: Belser/Epiney/Waldmann, § 9 N 35.

67 Vgl. im Zusammenhang mit der Gesichtserkennung Simmler/Canova, Gesichtserkennung, 202.

68 So etwa die französische Grenzpolizei am Basler Flughafen, vgl. dazu Braun Binder/Kunz/Obrecht, Rz. 10 m.w.H.

glichen werden sollen, ihrerseits ursprünglich zu einem anderen Zweck als der Strafverfolgung erstellt wurden.[69] Entsprechend stellt sich bei der automatisierten Informationsverarbeitung nicht nur die Frage der Befugnis zur Erhebung bestimmter Daten an sich. Vielmehr muss sich die Frage richtigerweise auch darauf beziehen, in welchem Umfang weitere Verarbeitungs- und Nutzungsmöglichkeiten zugelassen sind.[70]

Zusammengefasst bedarf es einer hinreichenden formell-gesetzlichen Grundlage, damit automatisierte Informationsverarbeitungsvorgänge zu Ermittlungs- und Strafverfolgungszwecken überhaupt zulässig sind.

IV. Rechtmässigkeit automatisierter Informationsbeschaffungsmethoden zu Strafverfolgungszwecken de lege lata

Bevor zu einer Analyse geschritten wird, ob die bestehenden strafprozessualen Rechtsgrundlagen den Einsatz von automatisierten Informationsbeschaffungsmethoden bereits hinreichend regeln, sei der Blick zunächst auf die im Zusammenhang mit automatisierten Informationsbeschaffungsmethoden ergangene bundesgerichtliche Rechtsprechung zu richten.

1. Automatisierte Informationsbeschaffungsmethoden im Lichte der bundesgerichtlichen Rechtsprechung

Der Blick auf die einschlägige höchstrichterliche Rechtsprechung beleuchtet, dass das Bundesgericht strenge Anforderungen an die Zulässigkeit automatisierter Informationsbearbeitungssysteme stellt. So stellte das Bundesgericht in zwei jüngeren Leitentscheiden[71] fest, dass die AFV zu einem schweren Eingriff in das Recht auf informationelle Selbstbestimmung führe, da sie sich nicht auf eine blosse Erhebung und Aufbewahrung von erkennungsdienstlichen Informationen beschränke.[72] Die serielle und simultane Verarbeitung grosser und komplexer Datensätze und die Möglichkeit der beliebigen Kombination mit anderen Datensätzen führe insgesamt zu einer erheblichen Eingriffsintensität. Diese nehme mit dem Zugriff auf die Daten und der Nutzung der Da-

69 Vgl. hierzu auch SIMMLER/CANOVA, „Smarte" Polizeiarbeit, 112.

70 Vgl. in diesem Sinne auch WESSLAU, 689 f.

71 BGE 149 I 218 und BGE 146 I 11.

72 BGE 146 I 11 E. 3.2; vgl. auch BGE 149 I 218 E. 8.11.4; siehe zum Ganzen auch BÜRGE, 58; SIMMLER/CANOVA, Gesichtserkennung, 210.

ten durch die zuständigen Behörden weiter erheblich zu. Namentlich könne die Kombination mit anderweitig erhobenen Daten und eine entsprechende Streuweite des Systems die Grundlage für Persönlichkeits- oder Bewegungsprofile bilden.[73] Aufgrund der schweren Eingriffsintensität dürfe die automatisierte Fahrzeugfahndung daher nur zum Schutz von Rechtsgütern und öffentlichen Interessen von erheblichem Gewicht eingesetzt werden.[74] Zudem müsse für die betroffene Personen erkennbar sein, ob und welche Informationen gesammelt und aufbewahrt und mit anderen Datensätzen verknüpft bzw. abgeglichen werden.[75] In beiden Urteilen kam das Bundesgericht im Ergebnis zum Schluss, dass die jeweiligen Bestimmungen im kantonalen Polizeirecht den Anforderungen an eine gesetzliche Grundlage für die AFV derzeit nicht hinreichend entsprechen.[76]

Auch in Bezug auf den nicht ausdrücklich im Gesetz geregelten Antennensuchlauf im Rahmen einer Rasterfahndung[77] äusserte sich das Bundesgericht bereits zu dessen Zulässigkeitsvoraussetzungen.[78] Zunächst müsse der *dringende Tatverdacht hinsichtlich eines Verbrechens* bestehen. Der Antennensuchlauf solle zudem in Anlehnung an Art. 273 Abs. 1 StPO i.V.m. Art. 269 Abs. 1 lit. c StPO nur *subsidiär* i.S. einer *ultima ratio* zur Anwendung gelangen. Da sich der Antennensuchlauf zwangläufig gegen eine noch unbekannte Täterschaft richtet, lässt das Bundesgericht „die mögliche Individualisierbarkeit der Zielperson gemäss Raster- bzw. Schnittmengenergebnis" genügen.[79] Schliesslich ist gemäss Bundesgericht im Sinne der Verhältnismässigkeit des Eingriffs erforderlich, dass bereits vorab mit einer *voraussichtlich kleinen Datenschnittmenge* zu rechnen ist,[80] mithin, dass sich die Ermittlungen bereits auf nur einige wenige Zielpersonen konzentrieren.[81] Da die abzugleichenden Daten zunächst in *anonymisierter* Form erhoben und abgeglichen werden und einzelne Personen erst identifiziert werden, wenn sie in das Fahndungsraster an ver-

---

73 Zum Ganzen 146 I 11 E. 3.2.

74 BGE 149 I 218 E. 8.7.

75 Vgl. BGE 146 I 11 E. 3.3.2.

76 Siehe BGE 146 I 11 E. 3.2 und E. 3.3 (Kanton Thurgau); BGE 149 I 218, Regeste sowie E. 8.5.2 (Kanton Solothurn).

77 Vgl. BGE 137 IV 340 E. 6.1.

78 BGE 137 IV 340 E. 6; vgl. zum Ganzen auch Biaggini, Rz. 205 ff.; Rz. 208.

79 BGE 137 IV 340 E. 5.6. Kritisch zum Kriterium der möglichen Individualisierbarkeit Biaggini, Rz. 191; Roos/Jeker, 179.

80 Siehe BGE 137 IV 340 E. 6.1; vgl. dazu Roos/Jeker, 180 f.; Gless/Geth, 1037.

81 Hansjakob, Antennensuchläufe, Rz. 13.

dächtigen Personen fallen,[82] erblickt das Bundesgericht in der Massnahme inklusive Schnittmengenbildung selbst indes noch keinen schweren Eingriff in die Privatsphäre.[83]

2. Keine hinreichende Gesetzesgrundlage de lege lata

In der Strafprozessordnung selber werden automatisierte Informationsverarbeitungsvorgänge zwecks Beweisgewinnung wie der Antennensuchlauf, die automatisierte Fahrzeugfahndung und Verkehrsüberwachung (AFV) und Gesichtserkennungstechnologien nicht als eigenständige strafprozessuale Zwangsmassnahme aufgeführt. Teilweise wird die Rechtmässigkeit dieser neuen Formen der Informationsverarbeitung jedoch unter Verweis auf bereits bestehende strafprozessuale Normen bejaht. Bei näherer Betrachtung wird jedoch ersichtlich, dass diese die Anforderungen nicht erfüllen, welche Art. 13 Abs. 2 BV an den Bestimmtheitsgrad und die Normdichte stellt.

a) Unzulässige Ausweitung bestehender Zwangsmassnahmen

In Bezug auf den Antennensuchlauf wird zuweilen die Auffassung vertreten, dieser stelle eine besondere Anwendungsform der rückwirkenden Randdatenerhebung nach Art. 273 StPO dar.[84] Indes gestattet dieser lediglich die einfache Randdatenerhebung für eine individualisierte konkrete Person.[85] Beim Antennensuchlauf werden indessen die Randdaten einer vorab unbestimmten Vielzahl von Personen simultan verarbeitet und ausgewertet.[86] Auch werden die weiteren Bearbeitungsschritte (Zusammenführen der erhobenen Daten zwecks Schnittmengenbildung sowie deren Abgleich anhand weiterer ermitt-

---

82 BGE 137 IV 340 E. 6.4 und E. 6.5; siehe auch FORSTER, 359.

83 Vgl. BGE 137 IV 340 E. 6.5.

84 HANSJAKOB, Antennensuchläufe, Rz. 24 m.w.H.; ähnlich HANSJAKOB, Überwachungsrecht, Rz. 437; unter Art. 273 StPO diskutiert als „besondere Überwachungsart" bei ZK StPO-HANSJAKOB/PAJAROLA, Art. 273 N 19; BSK StPO-JEAN-RICHARD-DIT-BRESSEL, Art. 273 N 6; vgl. auch die Botschaft zum aBÜPF 2013, 2749.

85 Vgl. so auch BGE 137 IV 340 E. 5.2, E. 5.4; ROOS/JEKER, 179; dazu bereits auch BIAGGINI, Rz. 195 f. m.w.H.

86 So scheidet Art. 273 StPO auch gemäss Bundesgericht als gesetzliche Grundlage aus, siehe BGE 137 IV 340 E. 5. Dass die jeweilige Zielperson zumindest individualisierbar sei, da sie durch die Standortdaten bereits feststehe und nur noch ermittelt werden müsse, weshalb Art. 273 StPO eine hinreichende Gesetzesgrundlage darstellen könne, überzeugt nicht, zumal diese Argumentation auf das Ergebnis des Antennensuchlaufs abstellt, siehe dazu im Einzelnen BIAGGINI, Rz. 196 f. m.w.H.; ROOS/JEKER, 179.

lungsrelevanter Erkenntnisse) von Art. 273 StPO nicht erfasst. Ebenso fehlt es an einer gesetzlichen Regelung, mit welchen Datenbanken und Registern die erfassten Datensätze abgeglichen werden dürfen. Zusammenfassend weist Art. 273 StPO nicht den hinreichenden Bestimmtheitsgrad auf, um als Gesetzesgrundlage für den Antennensuchlauf zu dienen.[87]

Unter Verweis auf die in Art. 260 StPO geregelte erkennungsdienstliche Erfassung einer Person bejaht etwa KÜHNE die Rechtmässigkeit des Einsatzes automatisierter Gesichtserkennungstechnologien im Strafverfahren.[88] Ähnlich wie bei der Randdatenerhebung liesse sich, wenn überhaupt, in Art. 260 StPO lediglich eine Grundlage für die Erfassung und biometrische Vermessung der Gesichtsmerkmale *einer einzelnen* zu identifizierenden Person erblicken.[89] Kernstück der automatisierten Gesichtserkennung bildet indessen nicht die Erfassung des einzelnen Gesichts als solches, sondern deren maschineller Abgleich mit anderen Datenbanken.[90] Bereits aufgrund der unbestimmten Anzahl an betroffenen Personen, die in den Datenerhebungs- und Verarbeitungsvorgang einbezogen werden, sowie der weitreichenden Möglichkeiten des Datenabgleichs kann Art. 260 StPO mangels Bestimmtheit nicht als hinreichende gesetzliche Grundlage genügen.[91]

Bezüglich der AFV erachtete das Bundesgericht die Bestimmungen in den jeweils zu beurteilenden kantonalen Polizeigesetzen wie dargelegt als unzureichend.[92] Ohnehin ist diskutabel, ob eine polizeirechtliche Rechtsgrundlage für die strafprozessuale Verwertbarkeit der hieraus erlangten Informationen überhaupt genügen würde oder ob es vielmehr einer (zusätzlichen) Rechts-

---

87 Siehe bereits BIAGGINI, 198 m.w.H. Ebenso wenig vermag die in Art. 66 Abs. 1 VÜPF und damit lediglich auf Verordnungsstufe enthaltene Begriffserläuterung des Antennensuchlaufs als hinreichende gesetzliche Grundlage genügen, dazu BIAGGINI, Rz. 192.

88 KÜHNE, 22. Auch der Bundesrat verneint unter Verweis auf Art. 260 f. StPO (für die Erfassung erkennungsdienstlicher Daten), Art. 354 Abs. 1 StGB (für deren Speicherung) und Art. 14 Abs. 2 des Bundesgesetzes über die polizeilichen Informationssysteme (BPI) die Notwendigkeit einer gesetzlichen Grundlage für den Einsatz von *Gesichtsbildabgleichen* zur Identifizierung einer Person im Strafverfahren, vgl. Interpellation Marti 22.3993, „Rechtliche Grundlage für die automatisierte Gesichtserkennung in Strafverfahren".

89 Vgl. dazu auch SIMMLER/CANOVA, Gesichtserkennung, 213.

90 Vgl. hierzu auch SIMMLER/CANOVA, Gesichtserkennung, 213; für die AFV BGE 146 I 11 E. 3.2.

91 Ebenso SIMMLER/CANOVA, Gesichtserkennung, 213. Selbiges muss mangels Normdichte auch für Art. 260 f. StPO i.V.m. Art. 354 StGB gelten, dazu im Einzelnen SIMMLER/CANOVA, Gesichtserkennung, 215 ff.

92 Vgl. Kap. IV.1.

grundlage in der Strafprozessordnung selbst bedarf.[93] Während sich im Bereich der doppelfunktionalen Aufgabenerfüllung der Polizei argumentieren lässt, dass hier stets auch eine Verwendung zu Strafverfolgungszwecken vom Zweck mitumfasst ist,[94] bedarf es jedenfalls bei einer ursprünglich zu rein präventiven Zwecken eingesetzten Informationsbeschaffungsmassnahme einer zusätzlichen expliziten Zweckumwidmungsnorm, welche die Verwendung zu repressiven Zwecken gestattet.[95]

b) Rückgriff auf allgemeine Datenbearbeitungsgrundsätze nach Art. 95 ff. StPO unzureichend

Zuweilen wird die Zulässigkeit der automatisierten Informationsbearbeitung zum Zwecke der Strafverfolgung auch gestützt auf Art. 95 ff. StPO bejaht.[96] Diese statuieren jedoch lediglich allgemeine Grundsätze der Beschaffung und Bearbeitung von Personendaten im Rahmen hängiger Strafverfahren sowie deren Bekanntgabe zwecks Verwendung in anderen hängigen Verfahren. Bereits mangels Bestimmtheit und Regelungsdichte können die in Art. 95 ff. StPO statuierten allgemeinen Grundsätze nicht als hinreichende Gesetzesgrundlage für neue Formen von Informationsverarbeitungsvorgängen mit der Intensität strafprozessualer Zwangsmassnahmen oder als Grundlage der Beweisverwertung dienen.[97] Während eine einfache „Google"-Suche durch die Strafverfolgungsbehörden noch von Art. 95 StPO abgedeckt sein mag,[98] so genügt dieser den verfassungsrechtlichen Anforderungen an eine hinreichende Gesetzesgrundlage für komplexe mehrstufige automatisierte Informationsverarbeitungsvorgänge nicht.

V. Anforderungen an die normative Ausgestaltung

Der Entwicklungsdynamik von strafprozessual zulässigen Formen der punktuellen Informationserhebung wie etwa von Randdaten (Art. 273 StPO) oder erkennungsdienstlichen Daten (Art. 260 StPO) hin zu komplexen automatisierten In-

---

93 Vgl. dazu Bürge, 59 f.

94 Siehe hierzu Zimmerlin/Galella, 378; vgl. dazu auch Zimmerlin, 273.

95 Vgl. dazu bereits Kap. III.3; Biaggini, Rz. 386 und Rz. 388; Brunner/Kradolfer, 56 f.

96 So etwa als subsidiäre Rechtsgrundlage bei Kühne, 21.

97 So bereits Biaggini, Rz. 38 und Rz. 379; für die automatisierte Gesichtserkennung Simmler/Canova, „Smarte" Polizeiarbeit, 114; Simmler/Canova, ZSR 2023, 215; a.A. Kühne, 21.

98 So Cartner/Schweingruber, 993 f.; vgl. dazu auch Simmler/Canova, Gesichtserkennung, 214.

formationsverarbeitungssystemen sind durch den verfassungsrechtlichen Datenschutz nach Art. 13 Abs. 2 BV Grenzen gesetzt. Es konnte voranstehend festgestellt werden, dass automatisierte Informationsverarbeitungsmethoden zum Zwecke der Strafverfolgung einer hinreichenden formell-gesetzlichen Grundlage bedürfen, an welcher es de lege lata noch fehlt.[99]

Das Erfordernis einer hinreichenden Gesetzesgrundlage erschöpft sich jedoch nicht im Bestehen einer gesetzlichen Grundlage an sich.[100] Vielmehr sind bei deren Ausgestaltung weitere Determinanten beachtlich, die sich aus dem grundrechtlichen Datenschutz nach Art. 13 Abs. 2 BV ableiten lassen. Eine Verhältnismässigkeitsprüfung im Einzelfall und hierin die Beurteilung, ob die Massnahme im konkreten Anwendungsfall ein geeignetes, erforderliches und verhältnismässiges Mittel zur Aufklärung der Straftat darstellt, bleibt dabei nach wie vor unentbehrlich.

1. Gesetzliche Verankerung sämtlicher Bearbeitungsschritte sowie hinreichende Schutzvorkehrungen gegen Datenmissbrauch

Ausgangspunkt bildet das Erfordernis einer hinreichenden Gesetzesgrundlage, in welcher sämtliche Bearbeitungsschritte – von der Erhebung der Ausgangsdaten und der automatischen oder manuellen Auswertung der Daten bis hin zum Abgleich der Daten mit weiteren Datenbanken – mit hinreichender Bestimmtheit normiert sind.[101] Im Sinne der Transparenz muss es für die betroffenen Personen vorhersehbar sein, unter welchen Voraussetzungen welche Informationen[102] gesammelt und aufbewahrt werden und mit welchen Datenbanken diese verknüpft respektive systematisch abgeglichen werden dürfen.[103] Eine weitere Einschränkung hat im Hinblick darauf zu erfolgen, unter welchen Voraussetzungen automatisierte Informationsbeschaffungsmass-

---

99 So in Bezug auf die automatisierten Gesichtserkennung Simmler/Canova, Gesichtserkennung, 202. Für einen konkreten Vorschlag eines Verwertbarkeitskonzepts für Informationen aus Antennensuchläufen vgl. Biaggini, Rz. 468 ff.; zu den Ansprüchen an eine strafprozessuale Regelung für die automatisierte Gesichtserkennung Simmler/Canova, Gesichtserkennung, 223 f.

100 Biaggini, Rz. 362; ebenso Bertram, 139; vgl. hierzu auch BVerfG 65, 1 (44, 61 f.).

101 Vgl. dazu auch BGE 146 I 11 E.3.3.2; BGE 149 I 218 E. 8.5.1.

102 So etwa in Bezug auf die AFV, ob neben dem Kontrollschild noch weitere Informationen wie etwa Standort, Fahrtrichtung und Zeitpunkt erfasst werden.

103 Vgl. dazu im Zusammenhang mit der AFV BGE 146 I 11 E. 3.3.2; BGE 149 I 218 E. 8.5.1.

nahmen im Strafverfahren eingesetzt werden dürfen, so etwa, ob diese einzig zur Aufklärung von Verbrechen oder von Katalogtaten angeordnet werden dürfen.[104]

Darüber hinaus verlangt Art. 13 Abs. 2 BV nach hinreichenden Schutzvorkehrungen gegen Datenmissbrauch. Hierzu zählen namentlich hinreichende Bestimmungen zur Aufbewahrung, Löschung, Übermittlung[105] der Daten etwa an (ausländische) Behörden und die weitere Verwendung der erhobenen Daten.[106] Weiter muss die Informationsbeschaffungsmassnahme auch in zeitlicher Hinsicht hinreichend umrissen sein. Für den Antennensuchlauf orientiert sich die bundesgerichtliche Rechtsprechung am Deliktszeitraum.[107] Auch beim Einsatz von stationären AFV-Geräten ist regelmässig zu überprüfen, ob deren Einsatz am fraglichen Ort zum bisherigen Zweck und unter den bisherigen Umständen weiterzuführen, zu modifizieren oder zu beenden ist.[108] Schliesslich bedarf es namentlich angesichts der potentiellen Fehleranfälligkeit automatisierter Informationsverarbeitungssysteme Bestimmungen zum hinreichenden Rechtsschutz für die Betroffenen.[109]

2. Zweckbestimmung: Gradmesser der Verhältnismässigkeit

Von besonderem Interesse ist bei automatisierten Informationsverarbeitungsvorgängen angesichts der mannigfachen Nutzungsmöglichkeiten der einmal erhobenen Daten die Ausgestaltung der Zweckbestimmung. Denn der Eingriff in die Rechtspositionen der betroffenen Personen wird mit jedem weiteren Verwendungseingriff wie auch der Weitergabe der Daten an (ausländische) Behörden perpetuiert und intensiviert.[110] Je vielseitiger die späteren Verwendungseingriffe ausfallen, desto schwerer wiegt bereits die Eingriffsbelastung

---

104 Vgl. dazu für den Antennensuchlauf BGE 137 IV 340 E. 6.1; für die AFV BGE 146 I 11, E. 3.3.2; für die automatisierte Gesichtserkennung SIMMLER/CANOVA, Gesichtserkennung, 223.

105 Vgl. zur Übermittlung der Daten an Dritte EGMR, *Centrum för Rättvisa gegen Schweden* vom 25. Mai 2021, §262 und 275.

106 BGE 146 I 11 E. 3.3.1; ebenso BGE 149 I 218 E. 8.9.

107 In BGE 137 IV 340 E. 6.4 erachtete das Bundesgericht zwei Stunden als angemessen.

108 BGE 149 I 218 E. 8.3.2.

109 Vgl. dazu im Einzelnen BGE 149 I 218 E. 8.10; SIMMLER/CANOVA, Gesichtserkennung, 224. Zur periodischen Kontrolle des Einsatzes von AFV durch unabhängige Behörde als Kontrollmechanismus BGE 149 I 218 E. 8.11.2. Im Falle eines Nichttreffers erachtet das Bundesgericht ein Feststellungsgesuch i.S.v. Art. 25 Abs. 1 DSG als ausreichend, vgl. BGE 149 I 218 E. 8.10.2.

110 Vgl. dazu bereits BIAGGINI, Rz. 427; vgl. dazu auch BVerfGE 113, 348 (384); in diesem Sinne auch BGE 146 I 11 E. 3.2.

des Erhebungseingriffs.[111] Somit stellt die Ausgestaltung der Zweckbestimmung den Gradmesser der Verhältnismässigkeit bei der Zulassung von automatisierten Informationsbeschaffungsmassnahmen dar. Entsprechend muss auch der Fokus bei der Ausgestaltung der gesetzlichen Grundlage im Sinne der Verhältnismässigkeit auf der Regulierung der möglichen späteren Verwendungszwecke der erhobenen Daten liegen. Allfällige weitere Nutzungsmöglichkeiten der Informationen müssten bereits im Erhebungszeitpunkt feststehen, weil sich diese auf die Verhältnismässigkeit der Massnahme auswirken.[112]

Findet der Einsatz der automatisierten Informationsverarbeitung zum Zwecke der Strafverfolgung statt, erfolgt deren Anordnung als strafprozessuale Zwangsmassnahme verdachtsgestützt im Hinblick auf ein konkretes Strafverfahren. Da sich die Zweckbindung auf das spezifische anlassgebende Strafverfahren und nicht etwa auf die Strafverfolgung als solche bezieht, beschränkt sich die Verwertbarkeit der hieraus resultierenden Informationen somit auch nur auf dieses konkrete, anlassgebende Strafverfahren.[113] Sollen die im Rahmen automatisierter Informationsbeschaffungsmethoden erhobenen Informationen – so beispielsweise das Ergebnis eines Antennensuchlaufs – in anderem Sachzusammenhang, namentlich in einem anderen Strafverfahren verwendet werden dürfen, bedarf dies i.S. einer *Zweckumwidmung* einer ausdrücklichen gesetzlichen Legitimierung.[114]

Dabei gilt es zu beachten, dass der verfassungsrechtliche Datenschutz auch der zweckändernden Verwendung von Informationen Grenzen setzt. Für Daten, welche zu keinem Datentreffer führen und damit im Hinblick auf die konkret anlassgebende Straftat nicht erforderlich sind, verlangt bereits der Grundsatz der Datensparsamkeit,[115] dass diese „Nichttreffer" umgehend zu löschen sind.[116] Auch sog. „unechte Treffer", die sich erst im Nachgang als falsch herausstellen, sind im Sinne der Verhältnismässigkeit umgehend (gegebenenfalls manuell) zu löschen.[117] Selbst wenn die Erhebung der Daten an sich recht-

111 Vgl. dazu Biaggini, 427 m.w.H.; in diesem Sinne auch BGE 146 I 11 E. 3.2.

112 Vgl. dazu Kap. III.2.

113 Vgl. im Zusammenhang mit dem Antennensuchlauf bereits Biaggini, Rz. 508.

114 Biaggini, Rz. 511; vgl. hierzu auch Singelnstein, Funkzellenabfrage, 607.

115 Nach diesem dürfen Daten nur insoweit bearbeitet werden, als es für den Zweck der Datenbearbeitung notwendig ist; vgl. zur Datensparsamkeit als Ausfluss des Verhältnismässigkeitsprinzips zum aDSG SHK DSG-Baeriswyl, Art. 4 N 23; siehe weiterführend BSK DSG-Bühlmann/Reinle, Art. 6 N 220 ff.

116 So auch in Bezug auf die AFV BGE 146 I 11 E. 3.3.2; vgl. auch BGE 149 I 218 E. 8.2.1 und E. 8.9.1; im Zusammenhang mit dem Antennensuchlauf Biaggini, Rz. 232.

117 Vgl. dazu BGE 149 I 218 E. 8.9.1.

mässig erfolgen würde, geht mit deren Speicherung ein weiterer grundrechtsrelevanter Eingriff einher,[118] der sich gerade durch die Verknüpfung von Daten intensiviert.[119] Das Vorrätighalten dieser Daten für allfällige künftige Delikte verbietet sich hier aus Gründen der Verhältnismässigkeit.

Aber auch für Trefferfälle muss gesetzlich geregelt sein, inwiefern und wie lange diese aufbewahrt werden dürfen.[120] Eine weitere Verwendung dieser Informationen zu einem anderen als dem Erhebungszweck kommt angesichts der erheblichen Eingriffsintensität des Informationserhebungseingriffs überhaupt nur dann in Betracht, wenn eine *wertungsmässige Gleichheit* zwischen Erhebungs- und dem spätere Verwendungseingriff besteht.[121] Indes wirken sich weitere zulässige Verwendungsmöglichkeiten bereits zusätzlich auf die Intensität des Erhebungseingriffs aus.[122] Insgesamt erscheint es nach vorliegender Auffassung daher auch hier angezeigt, die Verwendung der Informationen einzig auf den Erhebungszweck zu beschränken und die Daten nach Abschluss des Verfahrens zu löschen. Somit sollte die jeweilige Gesetzesgrundlage vorsehen, dass die über die automatisierte Informationsbeschaffung erlangten Informationen einzig für die Aufklärung der Anlasstat verwendet werden dürfen und nach Abschluss des Verfahrens integral zu löschen sind.[123]

VI. Schlussbetrachtung

Neue technische Möglichkeiten der Informationsbeschaffung führen zu einer Entwicklungsdynamik im Bereich der bereits bestehenden Ermittlungsmethoden. Dieser Entwicklungsdynamik hin zu einer Ausweitung strafprozessualer Zwangsmassnahmen über den klaren Gesetzeswortlaut hinaus ist indes namentlich durch den in Art. 13 Abs. 2 BV verankerten grundrechtlichen Datenschutz klare Grenzen gesetzt. So stellt das Verfassungsrecht Vorgaben an die normative Ausgestaltung der hierin stattfindenden Informationsverarbeitungsvorgänge, welche vorangehend im Einzelnen konturiert wurden. Sollen

118 Ebenso Singelnstein, Funkzellenabfrage, 607.

119 Dazu im Einzelnen Biaggini, Rz. 512; vgl. auch Singelnstein, Verwendungsregeln, 856.

120 Siehe BGE 146 I 11 E. 3.3.2.

121 Siehe hierzu Biaggini, Rz. 392 m.w.H.; in diesem Sinne auch BGE 149 I 218 E. 8.9.2. Zum *hypothetischen Ersatzeingriff* als Beurteilungsmassstab für die Zulässigkeit von Zweckumwidmungen Biaggini, Rz. 393 ff., Rz. 399.

122 Vgl. dazu Kap. II.

123 So für den Antennensuchlauf bereits Biaggini, Rz. 513. Vgl. in Bezug auf die DNA-Massenuntersuchung Art. 9 Abs. 3 DNA-Profil-Gesetz; ZK StPO-Hansjakob/Graf, Art. 256 N 12.

diese neuen Formen der automatisierten Informationsbeschaffung zu Ermittlungszwecken im Strafverfahren zulässig sein, bedürfen sie jeweils einer eigenständigen strafprozessualen Rechtsgrundlage, die den Anforderungen an das Bestimmtheitsgebot hinreichend Rechnung trägt.[124] Kernstück eines Verwertbarkeitskonzepts und Gradmesser der Verhältnismässigkeit bilden eine hinreichende Zweckbestimmung und Zweckbindung der automatisiert erhobenen Informationen. Letztlich kann mit der Zweckbindung der Informationen an die Anlasstat auch dem *chilling effect*[125] automatisierter Überwachungsmassnahmen auf die Grundrechtsausübung des Einzelnen aufgrund des Gefühls der dauernden Überwachung und der potenziell mannigfachen Nutzungsmöglichkeiten zumindest bis zu einem gewissen Grad begegnet werden.

Literatur

Albers Marion, Informationelle Selbstbestimmung, Berlin/Baden-Baden 2005

Baeriswyl Bruno/Pärli Kurt, Datenschutzgesetz (DSG), Handkommentar, Bern 2015 (zit. SHK DSG-Bearbeiter/in)

Belser Eva Maria/Epiney Astrid/Waldmann Bernhard (Hrsg.), Datenschutzrecht. Grundlagen und öffentliches Recht, Bern 2011 (zit. Autor/in, in: Belser/Epiney/Waldmann)

Bertram Konstantin, Die Verwendung präventiv-polizeilicher Erkenntnisse im Strafverfahren, Diss., Baden-Baden 2009

Biaggini Elena, Verwertbarkeit verdachtsbegründender Informationen aus Fernmeldeüberwachungen im Strafverfahren. Vorschlag eines Verwertbarkeitskonzepts für Informationen aus der präventiven und repressiven Überwachung des Fernmeldeverkehrs auf strafprozessualer und verfassungsrechtlicher Grundlage, Diss., Zürich 2022

Biaggini Giovanni, BV Kommentar, Bundesverfassung der Schweizerischen Eidgenossenschaft, 2. A., Zürich 2017 (zit. G. Biaggini, OFK BV)

Blechta Gabor-Paul/Vasella David (Hrsg.), Basler Kommentar, Datenschutzgesetz/Öffentlichkeitsgesetz (DSG), 4. A., Basel 2024 (zit. BSK DSG-Bearbeiter/in)

Braun Binder Nadia/Kunz Eliane/Obrecht Liliane, Maschinelle Gesichtserkennung im öffentlichen Raum, sui-generis 2022, 53 ff.

Brunner Arthur/Kradolfer Matthias, Legistische Herausforderungen im Polizeirecht, Recht & Risiko 2/2023, 34 ff.

Bürge Lukas, Zulässigkeit und Verwertbarkeit von polizeilichen Aufzeichnungen der automatischen Fahrzeugfahndung und Verkehrsüberwachung (AFV), forumpoenale 1/2021, 56 ff.

124 So auch Simmler/Canova, Gesichtserkennung, 225.

125 Vgl. BGE 146 I 11 E. 3.2; grundlegend auch EGMR vom 27. März 1996 (GC), *Goodwin v. The United Kingdom*, no. 17488/90, §39.

Cartner Anna/Schweingruber Sandra, Strafbehörden dürfen googeln, AJP 2021, 990 ff.

Donatsch Andreas/Lieber Viktor/Summers Sarah/Wohlers Wolfgang, Kommentar zur Schweizerischen Strafprozessordnung (StPO), 3. A., Zürich 2020 (zit. ZK-StPO-Bearbeiter/in)

Ehrenzeller Bernhard/Schindler Benjamin/Schweizer Rainer J./Vallender Klaus A. (Hrsg.), Die Schweizerische Bundesverfassung, St. Galler Kommentar, 3. A., Zürich 2014 (zit. SGK BV-Bearbeiter/in)

Forster Marc, Antennensuchlauf und rückwirkende Randdatenerhebungen bei Dritten. Bundesgerichtspraxis und gesetzliche Lücken betreffend Art. 273 und Art. 270 lit. b StPO, in: Jositsch Daniel/Schwarzenegger Christian/Wohlers Wolfgang (Hrsg.), Festschrift für Andreas Donatsch zum 65. Geburtstag, Zürich 2017, 357 ff.

Gächter Thomas/Meier Michael E., Observation – ein Rechtsinstitut unter Beobachtung, in: Jusletter 11. Dezember 2017

Gächter Thomas/Werder Gregori, Einbettung ausgewählter Konzepte in das schweizerische Datenschutzrecht, in: Epiney Astrid/Fasnacht Tobias/Blaser Gaetan (Hrsg.), Instrumente zur Umsetzung des Rechts auf informationelle Selbstbestimmung/Instruments de mise en oeuvre du droit à l'autodétermination informationelle, Zürich 2013, 87 ff.

Gless Sabine, Predicitve policing und operative Verbrechensbekämpfung, in: Herzog Felix/Schlothauer Reinhold/Wohlers Wolfgang (Hrsg.), Rechtsstaatlicher Strafprozess und Bürgerrechte, Gedächnisschrift für Edda Wesslau, Berlin 2016, 169 ff.

Gless Sabine/Geth Christopher, Antennensuchlauf und Rasterfahndung, in: Kuhn André et al. (Hrsg.), Kriminologie, Kriminalpolitik und Strafrecht aus internationaler Perspektive, Festschrift für Martin Killias zum 65. Geburtstag, Bern 2013, 1033 ff.

Hansjakob Thomas, Überwachungsrecht der Schweiz, Kommentar zu Art. 269 ff. StPO und BÜPF, Zürich/Basel/Genf 2017 (zit. Hansjakob, Überwachungsrecht)

Hansjakob Thomas, Zur Zulässigkeit von Antennensuchläufen, Bemerkungen zu BGE 1B_376/2011 vom 3. November 2011, in: Jusletter 5. März 2012 (zit. Hansjakob, Antennensuchläufe)

Kühne Stefan, Automatisierte Bearbeitung von Personendaten im Polizei- und Strafprozessrecht, Sicherheit & Recht 2022, 13 ff.

Niggli Marcel Alexander/Heer Marianne/Wiprächtiger Hans (Hrsg.), Basler Kommentar, Schweizerische Strafprozessordnung/Jugendstrafprozessordnung (StPO/ JStPO), 3. A., Basel 2023 (zit. BSK StPO-Bearbeiter/in)

Simmler Monika/Canova Giulia, Die Unrechtmässigkeit des Einsatzes automatisierter Gesichtserkennung im Strafverfahren – ein weiterer Beitrag zu einer anhaltenden Debatte, ZSR Zeitschrift für Schweizerisches Recht 3/2023, 201 ff. (Simmler/Canova, Gesichtserkennung)

Simmler Monika/Canova Giulia. Gesichtserkennungstechnologie: die „smarte" Polizeiarbeit auf dem rechtlichen Prüfstand, Sicherheit & Recht 2021, 105 ff. (Simmler/Canova, „Smarte" Polizeiarbeit)

Singelnstein Tobias, Verhältnismässigkeitsanforderungen für strafprozessuale Ermittlungsmassnahmen – am Beispiel der neueren Praxis der Funkzellenabfrage, JZ 2012, 601 ff. (zit. Singelnstein, Funkzellenabfrage)

Singelnstein Tobias, Strafprozessuale Verwendungsregelungen zwischen Zweckbindungsgrundsatz und Verwertungsverboten. Voraussetzungen der Verwertung von Zufallsfunden und sonstiger zweckentfremdender Nutzung personenbezogener Daten im Strafverfahren seit dem 1. Januar 2008, in: ZStW 120 (2008), 854 ff. (zit. Singelnstein, Verwendungsregeln)

Roos Eveline/Jeker Konrad, Antennensuchlauf im Rahmen einer Rasterfahndung, forumpoenale 2012, 175 ff.

Waldmann Bernhard/Belser Eva Maria/Epiney Astrid (Hrsg.), Schweizerische Bundesverfassung (BV), Basel 2015 (zit. BSK BV-Bearbeiter/in)

Wesslau Edda, Gefährdungen des Datenschutzes durch den Einsatz neuer Medien im Strafprozess, ZStW 113 (2001), 681 ff.

Zimmerlin Sven, Nr. 27 Bundesgericht, Strafrechtliche Abteilung, Urteil vom 26. Oktober 2022 i.S. A. gegen Staatsanwaltschaft des Kantons Basel-Landschaft – 6B_1061/2020, forumpoenale 4/2023, 265 ff.

Zimmerlin Sven/Galella Marco, Aspekte der beweismässigen Verwertbarkeit von polizeirechtlich erhobenen Informationen im Strafverfahren, forumpoenale 5/2019, 374 ff.

RISIKO RECHT

2. Jahrgang

ERSCHEINUNGSWEISE

R&R – Risiko & Recht erscheint dreimal jährlich online. Die Ausgaben werden zeitgleich im Wege des print on demand veröffentlicht; sie können auf der Verlagswebseite (www.eizpublishing.ch) sowie im Buchhandel bestellt werden.

ZITIERWEISE

R&R, Ausgabe 1/2023, …

KONTAKT

EIZ Publishing
c/o Europa Institut an der Universität Zürich
Dr. Tobias Baumgartner, LL.M., Rechtsanwalt
Hirschengraben 56
8001 Zürich
Schweiz
eiz@eiz.uzh.ch

ISSN

2813-7841 (Print)
2813-785X (Online)

ISBN:

978-3-03805-705-5 (Print – Softcover)
978-3-03805-706-2 (PDF)
978-3-03805-707-9 (ePub)

VERSION

1.01-20240619

DOI

Zeitschrift: https://doi.org/10.36862/eiz-rrz01
Ausgabe: https://doi.org/10.36862/eiz-rr202402
Dirk Baier, Anstieg der Kriminalität in der Schweiz: Zur Bedeutung des Faktors Staatsangehörigkeit, https://doi.org/10.36862/eiz-rr202402-01
Elena Biaggini, Automatisierte Informationsverarbeitung im Strafverfahren: Hinreichende Zweckbestimmung als Gradmesser der Verhältnismässigkeit, https://doi.org/10.36862/eiz-rr202402-02

RISIKO

EIZ Publishing

Herausgeber:
Prof. Dr. Tilmann Altwicker
Prof. Dr. Dirk Baier
PD Dr. Goran Seferovic
Prof. Dr. Franziska Sprecher
Prof. Dr. Stefan Vogel
Dr. Sven Zimmerlin

RISIKO & RECHT AUSGABE 02 / 2024

RECHT