Ruhr- Universität Bochum

- Juristische Fakultät -

MASTER KRIMINOLOGIE KRIMINALISTIK UND POLIZEIWISSENSCHAFT

Masterarbeit im

Masterstudiengang „Kriminologie, Kriminalistik und Polizeiwissenschaft“

Ruhr-Universität Bochum

Eine kriminalistisch-juristische Analyse bildbasierter Ermittlungsmethoden. Gesichtserkennung und Öffentlichkeitsfahndung unter der Lupe.

Erstgutachterin: Regina Stuchlik

Zweitgutachter: Dr. Andreas Ruch

Vorgelegt von:

Anika Kepert
anikakepert@gmx.de

am 29.01.2018

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Aus Gründen der besseren Lesbarkeit wird in der folgenden Arbeit auf die gendergerechte Ausführung personenbezogener Bezeichnungen verzichtet. Alle Angaben beziehen sich auf Angehörige beider Geschlechter.

In dubio pro libertate?[1]

[1] Vgl. zum Meinungsstreit über die Existenz einer Rangfolge bzw. sogar Priorisierung von individuellen vor kollektiven Rechtsgütern *Alexy*, Aussprache und Schlussworte, 123. Übersetzung: Im Zweifel für die Freiheit?

1 Einleitung

„Durch technische Mittel (…) wird Privatheit im Dienste von Bestrebungen, innere Sicherheit herzustellen, konsequent aufgelöst.“[2] Privatheit ist Freiheit und sowohl Freiheit als auch Sicherheit sind Rechtsgüter in Form persönlicher Grundbedürfnisse.[3] Zwischen Freiheit und Sicherheit besteht ein Spannungsverhältnis. Diese beiden Bedürfnisse in Waage zu halten ist schwierig.[4] Das eine Bedürfnis für das andere aufzugeben ist inakzeptabel.

Im Zusammenhang von Technisierung und Sicherheit sind Videoüberwachungsanlagen und ihre Omnipotenz[5] ein politisches Dauerthema. In den letzten ein bis zwei Jahren gab es Ereignisse, die den Diskurs über den Einsatz und die Ausweitung von Videoüberwachung im öffentlichen Raum, trotz des bekannten Spannungsverhältnisses, weiter angeregt sowie letztlich sogar den Beschluss über entsprechende Gesetzespakete bewirkt haben.[6]

Der Flüchtlingsstrom Ende 2015 und die Silvesternacht im gleichen Jahr, in der es in mehreren deutschen Städten zu sexuellen Übergriffen und Diebstahlsdelikten kam, sind nur zwei davon. Diese zwei korrelierenden Begebenheiten führten dazu, dass das Vertrauen der Bürger in die Kompetenz des Staates, hinsichtlich seines Schutzauftrages, gelitten hat.[7] Die registrierten Straftaten in dieser Nacht wurden im Laufe ihrer Ermittlungsverfahren und Verhandlungen durch mangelhafte Videobeweise und Täteridentifizierungen zum Exempel dafür, dass die Technik keine Sicherheit garantiert.[8]

Vorkommnisse, wie publik gewordene, besonders rohe Körperverletzungsdelikte in Berliner U-Bahnstationen, trieben die Diskussion weiter an. Im Jahr 2016 wurden dort unter anderem ein Obdachloser angezündet und eine Frau die Treppe heruntergetreten.[9] Es ist immer wieder in den Medien zu sehen und zu lesen, dass Straftaten durch Videobeweise schnell aufgeklärt werden

---

2 *Dollinger/Schmidt-Semisch*, Sicherheit und Alltag: Einführende Zugänge, 3.
3 Vgl. *Klamt*, Verortete Normen, 117.
4 Vgl. *Andexinger*, Das Spannungsfeld Freiheit versus Sicherheit, 123.
5 Vgl. *Schnabel*, Die polizeiliche Videoüberwachung öffentlicher Orte in Niedersachsen, 879.
6 Vgl. *Geyer*, Frankfurter Rundschau, http://www.fr.de/politik/sicherheitspolitik-bringen-mehr-kameras-mehr-sicherheit-a-736538, (25.08.207); vgl. *Bundesregierung*, Bessere Videoüberwachung für mehr Sicherheit, https://www.bundesregierung.de/Content/DE/Artikel/2016/12/2016-12-21-bessere-videoueberwachung.html, (25.08.2017).
7 Vgl. *Sigmund*, Allein unter Feinden? 23.
8 Vgl. *Bundestag Drucksache,* 18/10137, 2f.; vgl. *Sigmund*, Allein unter Feinden? 23ff.
9 Vgl. *Mai*, Interaktive Karte. So gefährlich ist es auf Berlins U-Bahnhöfen, http://www.berliner-zeitung.de/berlin/verkehr/interaktive-karte-so-gefaehrlich-ist-es-auf-berlins-u-bahnhoefen-26177452, (25.08.2017).

konnten. Letztlich führten der Amoklauf in München am 22. Juli 2016 und der Terroranschlag am 19. Dezember 2016 auf einem Berliner Weihnachtsmarkt zu politischem Handlungsdruck, wobei die letztgenannten Begebenheiten ausschlaggebend für die Gesetzesänderung waren.[10]

Videoüberwachung ist in vielen Punkten diskutabel und wird bereits von verschiedenen Wissenschaftsbereichen thematisiert und untersucht. Bei *Rolfes* findet sich beispielsweise die Auseinandersetzung mit Videoüberwachung aus humangeografischer Perspektive.[11] *Belina* diskutiert im Zusammenhang mit Videoüberwachung räumliche Überwachungsstrategie und E-Government.[12] Eine sozialwissenschaftliche Untersuchung von *Kudlacek* erforscht auch aus kriminologischer Sicht die Akzeptanz von Videoüberwachung in der Bevölkerung und versucht zudem Ursachen für die Einstellungen zu finden.[13] Die wissenschaftlichen Stimmen sind kritisch. Aktuell gibt es seitens des Bundesinnenministers *De Maizière* trotzdem intensive Überlegungen zur Implementierung einer Gesichtserkennungssoftware an videoüberwachten Bereichen. Das Projekt „Sicherheitsbahnhof Berlin Südkreuz“ soll über sechs Monate intelligente Videoüberwachungssoftware testen. Softwarebasierte Systeme sollen Gesichter erfassen und mit einer Testdatenbank abgleichen, heißt es in einer Pressemitteilung des Bundesinnenministeriums am 01.08.2017.[14] Videoüberwachung hat folglich bereits kriminalpräventiv und strafprozessual Einfluss auf Polizeiarbeit und wird es in Zukunft voraussichtlich noch mehr haben. Videobeweise werden aus kriminalistischer Sicht unter anderem relevant, wenn sie zur Grundlage polizeilicher Ermittlungsarbeit bei bildbasierten Ermittlungsmethoden werden.

„Kriminalistisches Arbeiten ist Wahrheitsforschung“.[15] Es reicht daher nicht aus, eine Straftat zu erkennen. Tathergänge müssen hypothetisiert und später rekonstruiert, entsprechende Beweise erhoben, geprüft sowie letztlich verifiziert oder falsifiziert werden. Kriminalistische Wahrheitsforschung ist die Basis

---

10 Vgl. *Bundesregierung*, Bessere Videoüberwachung für mehr Sicherheit, https://www.bundesregierung.de/Content/DE/Artikel/2016/12/2016-12-21-bessere-videoueberwachung.html, (25.08.2017).
11 Vgl. *Rolfes*, Kriminalität, Sicherheit und Raum, 117-121.
12 Vgl. *Belina*, Sicherheit durch Technik? 115-127.
13 Vgl. *Kudlacek*, Akzeptanz von Videoüberwachung, 16f.
14 Vgl. *Bundesinnenministerium*, „Sicherheitsbahnhof Berlin Südkreuz“, Test von Gesichtserkennungstechnik am Bahnhof Berlin Südkreuz beginnt, http://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2017/08/gesichtserkennungstechnik-bahnhof-suedkreuz.html, (25.08.2017).
15 *Walder/Hansjakob*, Kriminalistisches Denken, 10.

strafprozessualer Entscheidungen. Sie bestimmt den Verfahrensausgang wesentlich. Nur ein lückenloser und zweifelsfreier Tatnachweis kann am Ende einer Gerichtsverhandlung zu einer Verurteilung des Tatverdächtigen führen.[16] Im Strafverfahren ist die Identifizierung des Beschuldigten auf dem Videoüberwachungsmaterial vom Tatort unter Umständen das bedeutendste Beweismittel. Identifizierung heißt, dass der Beschuldigte aufgrund eindeutiger charakteristischer Merkmale und unveränderbarer Muster zweifelsfrei als der Straftäter wiedererkannt werden muss.[17] Wenn das Beweismaterial aus Videoüberwachungsanlagen mangelhaft ist, so wie in den angesprochenen Kölner Ermittlungsverfahren, dann wird es untauglich für die Belastung eines Tatverdächtigen vor Gericht. Gelingt es nicht, die Staatsanwaltschaft oder den Richter restlos von der Täterschaft eines Beschuldigten zu überzeugen, gilt in Deutschland der rechtsstaatliche Grundsatz in dubio pro reo. Das Verfahren wird eingestellt oder endet in einem Freispruch.[18]

Die ebenfalls bereits genannten Straftaten in den Berliner U-Bahnhöfen Hermann- und Schönleinstraße konnten wiederum, mithilfe der Aufnahmen aus Videoüberwachungsanlagen in Verbindung mit Öffentlichkeitsfahndungen durch Hinweise aus der Bevölkerung, geklärt werden.[19] Dies weist auf das Potenzial der Öffentlichkeitsfahndung hin. Es stellt sich mithin aber auch die Frage, ob die Berliner Identifizierungen durch die Videobeweise die Ausnahme oder die Regel sind. Es besteht die Möglichkeit, dass diese (Einzel-)Fälle instrumentalisiert werden, um politische Interessen bei der Bevölkerung unter dem Deckmantel der Sicherheit durchzusetzen. Die Gunst der Gesellschaft soll für das Mittel der Videoüberwachung erlangt werden, die vielleicht überhaupt nicht so gut ist wie ihr Ruf.

Es soll in dieser Thesis untersucht werden, ob Videoüberwachung tatsächlich erheblich zur Aufklärung von Straftaten beiträgt oder ob sie und ihre Wirkung aus Sicht der Strafverfolgung überschätzt sind. Der Schwerpunkt dieser Arbeit

---

16 Vgl. *Walder/Hansjakob*, Kriminalistisches Denken, 10.
17 Vgl. *Thiel*, Identifizierung von Personen, 3.
18 Vgl. *Walder/Hansjakob*, Kriminalistisches Denken, 319f.
19 Vgl. *Metag/Bruns*, Zwei Straftaten aufgeklärt. Soso, lieber Senat, Kamera-Überwachung bringt also nichts, http://www.bz-berlin.de/berlin/friedrichshain-kreuzberg/soso-lieber-senat-kamera-ueberwachung-bringt-also-nichts, (26.08.2017).

wird daher auf der Kontextualisierung der Videoüberwachung mit den Ermittlungsmethoden der Gesichtserkennung und der Öffentlichkeitsfahndung liegen. Gesichtserkennung und Öffentlichkeitsfahndung gehören zu den wichtigsten bildbasierten Wiedererkennungs- und Ermittlungsverfahren.[20]

Es werden die Argumente verschiedener Wissenschaftsbereiche für und wider die Videoüberwachung dargestellt. Anschließend wird die Gesichtserkennung als Personenidentifizierungsverfahren beschrieben. Zunächst wird dazu ausgeführt, was sich hinter der Ermittlungsmethode Gesichtserkennung verbirgt und inwiefern sie bei der Strafverfolgung nützlich ist. Die Gesichtserkennung untergliedert sich in die Bereiche computergestützte Gesichtserkennung und Lichtbildvergleiche. Die Funktionsweise beider Methoden wird erläutert.

Eine weitere Identifizierungsmethode ist die erwähnte Öffentlichkeitsfahndung. Auch sie wird hinsichtlich ihrer Anwendungsmöglichkeiten und kriminalistischen Bedeutsamkeit beschrieben. Ferner wird auch auf die polizeiinternen Fahndungsnetzwerke eingegangen. Videoüberwachung, Gesichtserkennung und Öffentlichkeitsfahndung werden im Theorieteil dieser Thesis punktuell juristisch im Hinblick auf ihre Eingriffsintensität, Rechtsstaatlichkeit sowie datenschutzrechtliche Aspekte aufgearbeitet. Vor der Darstellung des empirischen Teils der Arbeit, wird ein Einblick in den nationalen und internationalen Forschungsstand der einzelnen Thematiken gegeben.

Die kriminalistische Analyse der vorgenannten Ermittlungsmethoden erfolgt durch die Untersuchung ihrer Bildquellen, deren Qualität und ihrer Effizienz. Es soll konkret erarbeitet werden, wie oft Gesichtserkennung und Öffentlichkeitsfahndung im Jahr 2016 in Hessen zur Identifizierung von Straftätern führten und auch wie groß der Anteil der Videobeweise daran war. Um fundierte Aussagen treffen zu können, werden vorab gezielte Forschungsleitfragen und Forschungshypothesen festgelegt, die über eine Sekundäranalyse prozessproduzierter Daten polizeiinterner Fallbearbeitung beantwortet werden. Dabei wird jeder hessische Fall von Gesichtserkennung und Öffentlichkeitsfahndung genau untersucht. Am Ende werden die Untersuchungsergebnisse separat abgebildet. Nach jedem Kapitel erfolgt ein Zwischenfazit, um die bisherigen Resultate zusammenzufassen.

---

[20] Vgl. *Averdiek-Gröner/Frings,* Standardmaßnahmen im Ermittlungsverfahren, 7.

Die Vielschichtigkeit und Vielseitigkeit des Themas sowie das Interesse verschiedener Wissenschaftsgebiete daran, zeigt, dass man den Untersuchungsgegenstand aus verschiedenen Perspektiven betrachten kann. Die Arbeit ist durch ihr Kernthema und den Bezug zu polizeilichen Ermittlungsmethoden schwerpunktmäßig kriminalistisch und soll ggf. einen Beitrag zur aktuellen Debatte darüber leisten, ob und inwiefern eine Ausweitung öffentlicher Videoüberwachung sinnvoll ist und vor allem, inwiefern sie einen Mehrwert für Strafverfolgungsbehörden darstellt. Die Arbeit schließt mit einer Diskussion über die Erkenntnisse und ihre möglichen sicherheitspolitischen Auswirkungen ab.

2 Grundlagen

2.1 Videoüberwachung

Die Geschichte der öffentlichen und polizeilich genutzten Bildübertragung beginnt in Deutschland mit stationären Fernsehkameras zur Überwachung von Verkehrsknotenpunkten in München in den Fünfzigerjahren. In den Sechziger- und Siebzigerjahren wurden dann bereits in verschiedenen großen Städten, quer durch die (westliche) Republik, schwenk- und steuerbare Kameras mit Zoom zur dauerhaften Beobachtung von Menschen, und nicht mehr nur des Verkehres, eingesetzt.[21] „Sicherheitstechnik im allgemeinen [sic!] ist ein Wachstumsmarkt und Videoüberwachung ein vielseitig einsetzbares Instrument nicht nur zur Prävention von Kriminalität und Terrorismus, sondern auch zum Gebäude- und Risikomanagement, zur Zugabfertigung, Buslinienüberwachung und Mauterhebung, um nur einige Bereiche zu nennen“, konstatieren *Hempel* und *Metelmann* bereits 2005, als hätten sie den „Sicherheitsbahnhof Berlin Südkreuz“ geahnt.[22] Auch Töpfer hält fest, dass sich die Anwendungsbereiche für Überwachungskameras seit den neunziger Jahren bis zum Anfang des 21. Jahrhunderts sowohl im privaten als auch im halböffentlichen und öffentlichen Raum weiter vervielfältigt haben. Dazu zählen der Einzelhandel, ebenso wie der öffentliche Personennahverkehr oder öffentliche Wege und Plätze.[23]

---

[21] Vgl. *Weichert*, Praxis und rechtliche Aspekte optischer Überwachungsmethoden – zum Einsatz moderner Videotechnik, 7ff.
[22] *Hempel/Metelmann*, Bild – Raum – Kontrolle, 10.
[23] Vgl. *Töpfer*, Die Kamera als Waffe? 257.

Anfang der 2000er erklärte man sich diese Entwicklung, neben dem rapiden technologischen Fortschritt,[24] mit einem kriminalpolitischen Paradigmenwechsel von der Betrachtung der Kriminalität als krankhafter sozialer Erscheinung zu einem unüberwindbaren Gesellschaftsphänomen, das entsprechend nur über solche Maßnahmen gehandhabt werden kann[25] und der Tatsache, dass Videoüberwachung im Sinne modernen City-Marketings zur Sicherheitsproduktion instrumentalisiert wird[26]. Wesentlich verantwortlich scheint daher ein gesamtgesellschaftlicher Wandel „vom Wohlfahrts- und Präventionsstaat hin zur Risiko-, Sicherheits- und Informationsgesellschaft“[27] zu sein. Daraus ließe sich mithin ableiten, dass neben der Kriminalprävention, vor allem die beweisgesicherte Strafverfolgung und die Aufwertung und Ordnung des urbanen Erscheinungsbildes durch staatliche und kommunale Überwachungsmaßnahmen bezweckt werden sollen.[28]

Belina schlussfolgert, dass durch den Zweck der Ordnungspolitik vermehrt Minderheiten und Randgruppen diskriminiert und verdrängt werden. Sie werden dadurch kriminalisiert, dass sie an einem Ort optisch nicht ins Bild passen. Sie sind nicht zur falschen Zeit am falschen Ort, sondern mit der falschen Kleidung, der falschen Hautfarbe oder dem falschen Habitus.[29] „Der Einsatz von Überwachungssystemen verändert die Formen der sozialen Kontrolle und die Strukturen sozialer Ungleichheit.“[30] Weiter kritisierte er, dass trotz empirischer Versuche zur Untersuchung positiver Effekte auf die Strafverfolgung, kaum Erfolgsmeldungen zu verzeichnen sind. Befürworter würden daher zunehmend auf den präventiven Wert der Videoüberwachung abstellen, obwohl dieser nachweislich nicht messbar sei. Er führt weiter an, dass Videoüberwachung ungeeignet ist, Einfluss auf die Motivation von Tätern zu nehmen und daher Straftaten auch nicht verhindern könne.[31]

„Bei der zum Zweck der Prävention eingesetzten Videoüberwachung öffentlicher Räume muss auf deren panoptischen Effekt gehofft werden, also darauf, dass die Betroffenen sich auch tatsächlich durch das Filmen gestört fühlen, ihr

---

[24] Vgl. *Töpfer*, Die Kamera als Waffe? 258.
[25] Vgl. *Töpfer*, Die Kamera als Waffe? 258; vgl. *Marx*, What’s New About The New Surveillance? 18f.; vgl. *McCahill*, Beyond Foucault: towards a contemporary theory of surveillance, 42.
[26] Vgl. *Töpfer*, Die Kamera als Waffe? 259.
[27] *Leopold*, Rechtskulturbruch, 284.
[28] Vgl. *Belina*, Raum, Überwachung, Kontrolle, 217ff.; vgl. *Belina*, Sicherheit durch Technik? 116.
[29] Vgl. *Belina*, Raum, Überwachung, Kontrolle, 213; 221; *Belina*, Sicherheit durch Technik? 124.
[30] *Apelt/Möllers*, Wie „intelligente“ Videoüberwachung erforschen? 590.
[31] Vgl. *Belina*, Raum, Überwachung, Kontrolle, 217f.

Verhalten den erwarteten Normen anpassen und gegebenenfalls die überwachten Räume verlassen“[32]. Dagegen wird argumentiert, dass sich die präventive Wirkung nicht auf den Antrieb des Täters bezieht, sondern lediglich auf das erhöhte Entdeckungsrisiko.[33] Der Vergleich von technischen Überwachungsmaßnahmen mit dem Konzept der Disziplinargesellschaft nach Foucault basierend auf dem Panopticon von Bentham, ist unter Wissenschaftlern weit verbreitet und wird schon seit Jahrzehnten genutzt, um Kritik zu üben.[34] Obgleich Foucault nicht von Videoüberwachung sprach, werden seitens der Kritiker häufig Parallelen zu seinem Buch ‚Überwachen und Strafen: Die Geburt des Gefängnisses‘ gezogen.[35] Ein solcher Vergleich mag in der Theorie zulässig sein, entsprechende Evidenzen gestalten sich jedoch, nicht zuletzt wegen der intrinsischen Motivationen, schwierig.[36]

Grundsätzlich lassen sich die Ziele der Videoüberwachung schon lange nicht mehr auf die drei genannten Schwerpunkte Prävention, Repression und Sicherheit durch Ordnung beschränken, zu unterschiedlich sind inzwischen die einzelnen Verwendungszwecke und vor allem die Einsatzmöglichkeiten.[37] „Grundlegend geht es bei der Videoüberwachung um die Überwachung von Menschen und Orten aus der Ferne, dauerhaft und objektiv. Dabei macht es allerdings einen bedeutenden Unterschied, ob es sich um ein System handelt, das aus nur einer Kamera und einem Bildschirm besteht, welche die Bilder eines umgrenzten Raumes aufnimmt und speichert (…), oder ob es sich um ein System vernetzter Kameras handelt, die aufzeichnen und gleichzeitig live beobachtet werden (…); oder ob es ein System ist, das außer den Kameras noch Abgleiche mit Datenbanken vorsieht und Technologien wie Gesichtserkennung o. ä. integriert.“[38]

Seit Beginn des neuen Jahrhunderts hat sich folglich in Bezug auf die technischen Möglichkeiten und die Einsatzgebiete viel getan. In akademischen Debatten und einschlägiger Literatur wird Videoüberwachung als Wundermittel

---

32 *Belina*, Raum, Überwachung, Kontrolle, 221.
33 Vgl. *Kudlacek*, Akzeptanz von Videoüberwachung, 32.
34 Vgl. *Klamt*, Verortete Normen, 126ff.; vgl. *Schroer*, Sehen, Beobachten, Überwachen, 334; vgl. *Rolfes*, Kriminalität, Sicherheit und Raum, 120.
35 Vgl. *Kudlacek*, Akzeptanz von Videoüberwachung, 20f.
36 Vgl. *Apelt/ Möllers*, Wie „intelligente“ Videoüberwachung erforschen? 589f.
37 Vgl. *Zurawski*, Videoüberwachung, 396.; vgl. *Flöther*, Überwachtes Wohnen, 52.
38 *Zurawski*, Videoüberwachung, 398.

deklariert.[39] *Schnabel* konstatierte hierzu 2011: „Bei der Videoüberwachung handelt es sich um eine sicherheitspolitische Wunderwaffe: Im Vergleich zu im Streifendienst eingesetzten Beamten ist sie relativ kostengünstig und soll das subjektive Sicherheitsgefühl stärken. Die Kameras ermöglichen häufig eine nachträgliche Aufklärung der Straftat, auch wenn ihr Einfluss auf die Begehung von Straftaten umstritten ist. Trotz gewichtiger Bedenken gegen die Effektivität im Rahmen der Gefahrenabwehr wird ihr Einsatz hartnäckig verteidigt und im Zweifelsfall ausgebaut.“[40]

In den Einsatz von Videoüberwachung wird offenkundig sehr viel Hoffnung gesetzt. Zum Einfluss der Videoüberwachung auf das Sicherheitsempfinden der Bevölkerung gibt es mehrere sozialwissenschaftliche und kriminologische Studien. Laut *Apelt* und *Möllers* besteht nach einer Analyse mehrerer Projekte zwar eine konstant hohe Akzeptanz (50 % - 90 %) gegenüber der Maßnahme in der Bevölkerung, diese Tatsache habe aber keinen entsprechenden Einfluss auf das subjektive Sicherheitsgefühl.[41] Argumentationen, die sich der Aussage bedienen, Videoüberwachung zu verstärken, um Sicherheitsgefühl zu produzieren, sind daher nicht ganz schlüssig.[42] Es scheint einen Unterschied zu machen, wo die Videoüberwachung installiert wird. Das subjektive Sicherheitsgefühl wird dann gestärkt, wenn es sich bei den überwachten Bereichen um Angsträume handelt. Videoüberwachung an unproblematischen Örtlichkeiten wirkt sich nicht auf das bürgerliche Empfinden aus.[43] Das subjektive Sicherheitsgefühl wird im Wesentlichen durch mediale Berichterstattung über Risiken geprägt.[44] „Wir leben in einer Epoche, in der die Risiken, von Naturkatastrophen, Armut oder Kriminalität betroffen zu sein, noch nie so gering waren, in der die empfundene Unsicherheit solchen Bedrohungen gegenüber aber sehr präsent ist.“[45] Das subjektive Sicherheitsgefühl sollte auch deshalb nicht Basis der Entscheidung über eine Ausweitung von Videoüberwa-

---

39 Vgl. *Rolfes*, Kriminalität, Sicherheit und Raum, 118; vgl. *Schnabel*, Die polizeiliche Videoüberwachung öffentlicher Orte in Niedersachsen, 879.
40 *Schnabel*, Die polizeiliche Videoüberwachung öffentlicher Orte in Niedersachsen, 879.
41 Vgl. *Apelt/Möllers*, Wie „intelligente“ Videoüberwachung erforschen? 587.
42 Vgl. *Rolfes*, Kriminalität, Sicherheit und Raum, 119.
43 Vgl. *Klauser*, Die Videoüberwachung öffentlicher Räume, 346; *Kubera*, Evaluation von Videoüberwachung in Bielefeld, 132f.
44 Vgl. *Apelt/Möllers*, Wie „intelligente“ Videoüberwachung erforschen? 588.
45 *Apelt/Möllers*, Wie „intelligente“ Videoüberwachung erforschen? 588.

chung sein, weil es definitorisch nicht unter den Begriff der öffentlichen Sicherheit fällt.[46] Die öffentliche Sicherheit umfasst im Sinne der Gesetze „das geschriebene und ungeschriebene objektive Recht (im wesentlichen Gesetze, Rechtsverordnungen, Satzungen, Gewohnheitsrecht), die rechtlichen Befugnisse und Schutzgüter des einzelnen Bürgers sowie die Einrichtungen und Veranstaltungen des Staates und der sonstigen Träger öffentlicher Gewalt“[47]. Weiterhin steht die teilweise enorme Akzeptanz im Widerspruch einer bisher ermittelten Effektivität. Dies ergibt sich einerseits daraus, dass die Ziele vielfältig und ex ante nicht eindeutig festgelegt sind[48] und andererseits daraus, dass zur spürbaren Kriminalitätsbekämpfung weitere polizeiliche Maßnahmen einhergehen müssen[49]. In Bezug auf die Akzeptanz von Videoüberwachung gibt *Kudlacek* in einer Untersuchung aus 2015 zu Bedenken, dass der Begriff „Akzeptanz“ mehrere Dimensionen hat und diese Tatsache bei Befragungen bisher wenig berücksichtigt wurde. Unter differenzierterer Betrachtung des Akzeptanzbegriffs, ergibt sich ein geringfügig weniger positives Bild der Einstellung der Bürger gegenüber der Maßnahme. Die Befürwortung geht dann bewiesenermaßen mit Besorgtheit einher.[50] Dabei schlägt sich diese Besorgtheit eher in Zweifeln über die Wirksamkeit nieder, als in unbestimmbaren Bedenken vor einer staatlichen Totalüberwachung.[51] Trotzdem: „Der Einsatz der Technik ist schließlich nur durch seinen direkten Nutzen zu rechtfertigen. Keinesfalls durch eine mehrheitliche Befürwortung. Forschung zur Akzeptanz von Technik kann daher auch nie Beschaffung von Legitimation sein.“[52]

Unterschiedliche Untersuchungen zur Wirkung der Videoüberwachung haben darüber hinaus unabhängig voneinander Zweifel ergeben.[53] In erster Linie wird ein Verdrängungseffekt der Kriminalität dokumentiert.[54] Es konnte empirisch belegt werden, dass Affekttaten oder Straftaten unter Alkoholeinfluss durch Videoüberwachung nicht verhindert werden können. Die grundsätzliche Annahme aber, dass Videoüberwachung dieses Potenzial besitzt, ist auch nicht

---

46 Vgl. *Pieroth et al.*, Polizei- und Ordnungsrecht, 123.
47 *Wirth*, Kriminalistik-Lexikon, 407.
48 Vgl. *Apelt/Möllers*, Wie „intelligente“ Videoüberwachung erforschen? 588.
49 Vgl. *Bornewasser/Schulz*, Systematische Videoüberwachung am Beispiel einer Maßnahme in Brandenburg, 75ff.
50 Vgl. *Kudlacek*, Akzeptanz von Videoüberwachung, 123; 147.
51 Vgl. *Kudlacek*, Akzeptanz von Videoüberwachung, 147.
52 *Kudlacek*, Akzeptanz von Videoüberwachung, 149.
53 Vgl. *Zurawski*, Videoüberwachung, 405ff; vgl. *Kubera*, Evaluation von Videoüberwachung in Bielefeld, 119ff.; vgl. *Eifler/Brandt*, Erfahrungen mit Videoüberwachung im Überblick, 95.
54 Vgl. *Klauser*, Die Videoüberwachung öffentlicher Räume, 348.

naiv.[55] Primär ist Videoüberwachung ermittlungsunterstützend und ergänzend und keine ultimative Überführungs- oder gar Präventionsmethode.[56]
Experten interpretieren Videoüberwachung, abgesehen von ihrer Wirkungsweise auch als strategische Konsequenz kriminalgeografischer Forschung und der Betrachtung von Kriminalität in Bezug auf ihren Raum.[57] Die Ausdifferenzierung von Kriminalität auf ihre Örtlichkeit und die optische Darstellung dieser Betrachtung durch Kartografie beispielsweise, lässt Kriminalität als gesamtgesellschaftliches Phänomen erscheinen, nicht als individuellen Fehltritt. Dies wiederum eröffnet neue Betrachtungsweisen und Interpretationsmöglichkeiten.[58] Im Vordergrund steht dann die Stigmatisierung des Raumes selbst als Brennpunkt oder Problemviertel.[59]
Es gibt auch Ansichten, die vertreten, dass Videoüberwachungsmaßnahmen militärisch intendiert sind und mithin rechtsstaatliche Prinzipien wie die Unschuldsvermutung und die Verhältnismäßigkeit verdrängen.[60] Dagegen spricht, dass die Unschuldsvermutung nicht durch staatliche Kontrolle entkräftet wird, sondern im Kern dem Schutz der Schwachen vor den Mächtigen dient.[61] Grundsätzlich zeigt sich, „technologische Entwicklungen werden entweder als Gefährdung oder als Chance unserer Zivilisation angesehen. Im Bereich der Strafverfolgung werden diese Entwicklungen besonders kritisch betrachtet, da Menschenwürde und Grundrechtsschutz oftmals unmittelbar tangiert sind.“[62]

2.2 Verrechtlichung, Rechtsstaatlichkeit und Datenschutz

Um dies insgesamt im Hinblick auf den vorliegenden Gegenstand besser beurteilen zu können, muss zunächst ein Blick auf die Verrechtlichung des Einsatzes von Videotechnik geworfen werden. Es muss dabei differenziert werden, ob die Überwachungsmaßnahme präventiv oder repressiv ist. Repressive Rechtsgrundlagen ergeben sich zum Beispiel aus der StPO, präventive

---

55 Vgl. *Kudlacek*, Akzeptanz von Videoüberwachung, 145.
56 Vgl. *Hempel*, Zur Evaluation von Videoüberwachung, 145.
57 Vgl. *Belina*, „Kriminalität“ und „Raum“. Zur Kritik der Kriminalgeographie und zur Produktion des Raumes, 129.
58 Vgl. *Belina*, Kriminalitätskartierung als Methode der Kritischen Kriminologie? https://halshs.archives-ouvertes.fr/halshs-01245026/document, 3f.
59 Vgl. *Rolfes*, Kriminalität, Sicherheit und Raum, 36.
60 Vgl. *Töpfer*, Die Kamera als Waffe? 269.
61 Vgl. *Stettner*, Sicherheit am Bahnhof, 103f.; vgl. *Heckmann*, Sicherheitsarchitektur im bedrohten Rechtsstaat, 18.
62 *Feltes*, Videoüberwachung. Es ist der Anfang…aber aller Anfang ist bekanntlich schwer, 181.

Rechtsgrundlagen ergeben sich aus dem jeweiligen Polizei- und Ordnungsrecht der Länder und des Bundes. Grundsätzlich werden in der Praxis häufig beide Zwecke gleichzeitig verfolgt, wodurch eine Mischform entsteht.[63]
Die präventive offene Datenerhebung von Bild- und Tonaufnahmen ist in jedem Bundesland rechtlich verankert.[64] Sinngemäß ist dort normiert, dass Polizei- und Ordnungsbehörden öffentlich zugängliche Räume videografieren und die Bildaufnahmen zudem aufzeichnen dürfen, „wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass Straftaten drohen".[65]
Das Besondere an den Befugnisnormen ist ihr Gefahrenbegriff. Hier wird keine konkrete Gefahr für die öffentliche Sicherheit oder Ordnung gefordert. Vielmehr soll schon im Vorfeld eingegriffen werden. Es handelt sich bei der präventiven Videoüberwachung somit um eine Maßnahme der Gefahrenvorsorge. Grundsätzlich bestehen keine verfassungsrechtlichen Bedenken dagegen, allerdings sollte eine restriktive Anwendung der Norm erfolgen und sich auf Kriminalitätsschwerpunkte begrenzen.[66]
Die präventive Videoüberwachung ist auch dann unbedenklich, wenn sie eine potenzielle Strafverfolgung in der Zukunft erleichtern soll, problematischer ist die Form der Videoüberwachung, bei der das gewonnene Datenmaterial automatisch abgeglichen wird.[67] Hierzu erfolgt eine ausführlichere Betrachtung unter dem Punkt 3.4. Das BVerfG hat die Verfassungsmäßigkeit der öffentlichen Videoüberwachung zur Gefahrenvorsorge unter Berücksichtigung des Übermaßverbotes bestätigt.[68] Das Übermaßverbot ist eine Form der Verhältnismäßigkeit und leitet sich aus dem Rechtsstaatsprinzip ab. Es besagt einerseits, dass ein Grundrechtseingriff durch den Staat einer Rechtsgrundlage bedarf. Das Eingreifen darf andererseits die individuellen Rechte des Betroffenen auch nur soweit einschränken, wie es notwendig ist, um öffentliche Interessen zu schützen.[69] § 20 g I, II BKAG fällt seinem Wortlaut nach ebenfalls unter prä-

63 Vgl. *Belina*, Raum, Überwachung, Kontrolle, 215.
64 Vgl. § 14 III HSOG; §§ 24, 24a, 24b ASOG Bln; § 31 BbgPolG; § 8 HmbPolDVG; § 21 PolG (BaWü); § 32 PAG (Bayern); § 29 BremPolG; §§ 15, 15a, 15b PolG NRW; § 32 SOG M-V; § 32 NdsSOG; § 27 POG (Rheinland-Pfalz); § 27 SPolG; § 37 SächsPolG; § 16 SOG LSA; § 184 LVwG (Schleswig-Holstein); § 33 PAG (Thüringen).
65 Vgl. dazu exemplarisch den Wortlaut gem. § 14 III HSOG.
66 Vgl. Urteil *VGH BW* vom 21.07.2003, Az. 1 S 377/02, Rn. 65.
67 Vgl. *Bäcker*, Kriminalpräventionsrecht, 420.
68 Vgl. *BVerfG*, Videoüberwachung öffentlicher Plätze, 688.
69 Vgl. *Katz*, Staatsrecht, 106f.

ventivpolizeiliche Ermächtigungsgrundlagen, die den Einsatz einer Videoüberwachung erlauben, wenn „Tatsachen die Annahme rechtfertigen“, dass bestimmte Straftaten begangen werden sollen.[70] Es geht hierbei nicht um die Überwachung öffentlicher Räume und somit um den Eingriff in die Grundrechte einer Vielzahl von Personen, sondern Einzelner.[71] Gleiches gilt für die Befugnisnorm aus § 28 I, II BPOLG.

Bei der repressiven Verankerung des Einsatzes technischer Mittel im Gesetz, geht es dann ebenfalls um einzelne Betroffene bzw. Beschuldigte. „Die Strafprozessordnung enthält keine Ermächtigung zu einer dauerhaften stationären Videoüberwachung.“[72]

Die Befugnis der Videoüberwachung einzelner Personen zur Strafverfolgung ergibt sich aus § 100 h StPO. Der Unterschied zum präventiven Einsatz liegt auch darin, dass der repressive Einsatz verdeckt und nicht offen erfolgt.[73] Weiterhin sind gem. § 100 h I S. 1 StPO Bildaufnahmen nur zulässig, wenn keine andere Ermittlungsmethode erfolgversprechend wäre. Die Befugnisse aus § 100 h StPO sind somit subsidiär und unterliegen im Gegensatz zur präventiven Gesetzgebung einer weiteren erheblichen Einschränkung.[74] „Subsidiaritätsregelungen sollen damit gewährleisten, dass bestimmte Ermittlungsmaßnahmen nur als ultima ratio eingesetzt werden.“[75]

Es gibt einen juristischen Streit über die Gesetzgebungskompetenzen von Bund und Ländern für den Fall, der Mischformen der Videoüberwachung, sprich für die Einrichtungen, deren Schwerpunkt nicht nur ein Aspekt der Gefahrenvorsorge ist, sondern wo Bildaufnahmen oder -aufzeichnungen auch der Strafverfolgungsvorsorge dienen sollen.[76] Die wesentlichen Argumente dazu wurden bereits erläutert. Eigentlich fällt die Ausgestaltung der Strafverfolgung und die Gesetzgebung zum Verfahren in die Kompetenz des Bundes und ergibt sich aus Art. 74 I Nr. 1 GG. Gefahrenabwehr und Gefahrenvorsorge sind Ländersache. Da der Gesetzgeber aber bisher darauf verzichtet hat entsprechende Gesetze für eine Strafverfolgungsvorsorge zu erlassen, bestehen

---

70 Vgl. *Bäcker*, Kriminalpräventionsrecht, 238.
71 Vgl. *Bäcker*, Kriminalpräventionsrecht, 421.
72 *Bäcker*, Kriminalpräventionsrecht, 420f.
73 Vgl. *Belina*, Raum, Überwachung, Kontrolle, 214.
74 Vgl. *Joecks,* Studienkommentar StPO, Rn. 4, 225.
75 *Bäcker*, Kriminalpräventionsrecht, 147.
76 Vgl. *Schnabel*, Die polizeiliche Videoüberwachung öffentlicher Orte in Niedersachsen, 881.

nach herrschender Meinung keine kompetenzrechtlichen Bedenken.[77] Die Videoüberwachung sorgt jedoch auch materiellrechtlich für Streit. Zu Beginn der Einführung der Videoüberwachung öffentlicher Räume wurde in der Überwachungsmaßnahme kein Grundrechtseingriff gesehen. Erst die Aufzeichnung des Materials sei ein Eingriff in die Freiheitsrechte.[78] Das BVerfG stellte später, aufgrund einer Verfassungsbeschwerde, in einem Urteil über die Videoüberwachung öffentlicher Plätze fest, dass diese Form der Videoüberwachung in das allgemeine Persönlichkeitsrecht, speziell in das Recht auf informationelle Selbstbestimmung gem. Art. 2 I GG i. V. m. Art. 1 I GG von Passanten eingreift. Von der Bekanntgabe und Offenheit der Maßnahme darf auch nicht automatisch auf eine Einwilligung zur Informationserhebung der Betroffenen geschlossen werden.[79] Das Recht auf informationelle Selbstbestimmung ist nicht explizit im Grundgesetz normiert. Es wurde durch das BverfG in dem sog. Volkszählungs-Urteil aus dem allgemeinen Persönlichkeitsrecht abgeleitet und besagt, dass personenbezogene Daten nicht willkürlich erhoben, gespeichert und verarbeitet werden dürfen, sondern dass jeder Einzelne das Recht hat über den Umgang mit seinen Daten frei zu entscheiden.[80]

Durch das Kamera- Monitor-Prinzip ist es einfacher, gezielt einzelne Personen zu beobachten, sie ranzuzoomen und zu individualisieren.[81] Es eröffnen sich dadurch Möglichkeiten, die über eine unspezifische, allgemeine Beaufsichtigung hinausgehen.[82] Während dieses Prinzip unstreitig in Grundrechte eingreift, wurde später ebenfalls gerichtlich entschieden, dass auch schon bei der reinen Überwachung von einem Grundrechtseingriff ausgegangen werden muss. Unabhängig davon, ob bereits eine Nahaufnahme erfolgt bzw. möglich ist.[83] Argumentum a fortiori wird durch die öffentliche Videoüberwachung in die allgemeine Handlungsfreiheit gem. Art. 2 I GG eingegriffen. Das Wissen über die Aufzeichnung oder die reine Möglichkeit des Beobachtetwerdens übt auf Passanten einen latenten Verhaltenszwang in Form eines Anpassungsdrucks

---

77 Vgl. *Schenke*, Polizei- und Ordnungsrecht, 112; vgl. VGH BW vom 21.07.2003, Az. 1 S 377/02, Rn. 34; vgl. *BVerwG* vom 25.01.2012, Offene Videoüberwachung der Reeperbahn, 759f.

78 Vgl. *VG Halle*, Videoüberwachung eines öffentlichen Platzes, 164; vgl. *VG Karlsruhe*, Videoüberwachung öffentlicher Räume, 117f.

79 Vgl. *BVerfG*, Videoüberwachung öffentlicher Plätze, 688; vgl. zum konkludenten Grundrechtsverzicht auch *VGH BW* vom 21.07.2003, Az. 1 S 377/02, Rn. 43.

80 Vgl. *BVerfG*, Verfassungsrechtliche Überprüfung des Volkszählungsgesetzes 1983, 419.

81 Vgl. insbesondere im Zusammenhang mit dem Grundrechtseingriff *Gusy*, Die „Schwere“ des Informationseingriffs, 401f.

82 Vgl. *Schenke*, Polizei- und Ordnungsrecht, 113.

83 Vgl. *VGH BW* vom 21.07.2003, Az. 1 S 377/02, Rn. 39f.

aus, weshalb sie sich nicht mehr frei entfalten können.[84] Dies lässt sich sinngemäß auch aus dem Volkszählungsurteil entnehmen. Dort steht: „Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen."[85]

Im Rahmen der Verhältnismäßigkeit wird geprüft, wann und wie die Rechte des Einzelnen den Anspruch der Allgemeinheit auf (Innere und Äußere) Sicherheit überwiegen und umgekehrt. Freiheit und Sicherheit begleitet folglich naturgemäß ein Spannungsverhältnis, obwohl die Freiheit die Sicherheit gleichermaßen auch benötigt. Denn nur wer sicher ist, kann sich frei bewegen.[86] Insofern kann man von einem dichotomen Verhältnis sprechen.[87] Bei der Verrechtlichung von Videoüberwachung ist daher immer der „rechtsstaatliche Balanceakt" zu bedenken, „Freiheit gegen Sicherheit abwägen, Sicherheit für Freiheit aufgeben, Freiheit für Sicherheit einschränken"[88]. Dieser Drahtseilakt wird nicht nur kontrovers diskutiert, sondern die Aspekte Freiheit und Sicherheit werden von Zeit zu Zeit, nicht nur einzelfallbezogen, auch unterschiedlich gewichtet. Hieß es beispielsweise 1983 im Volkszählungsurteil: „Das Grundgesetz hat, wie in der Rechtsprechung des BVerfG mehrfach hervorgehoben ist, die Spannung Individuum - Gemeinschaft im Sinne der Gemeinschaftsbezogenheit und Gemeinschaftsgebundenheit der Person entschieden"[89] und in einer Bundestagsdrucksache aus 2006 zur Vorratsdatenspeicherung in Zusammenhang mit Strafverfolgung und Grundrechtsschutz noch: „Grundrechte sind jedoch nicht vorbehaltlos gewährleistet. Ihre gesetzliche Einschränkung ist zur Verfolgung vernünftiger Gemeinwohlbelange, wie etwa der Gewährleistung einer wirksamen Strafverfolgung in bestimmten Kriminalitätsbereichen, zulässig"[90], kippte das BVerfG kurze Zeit später die Regelungen zur Vorratsdatenspeicherung und entschied mithin gegenteilig im Sinne der Freiheitsrechte des Einzelnen, dass die Ausgestaltung des neuen

---

84 Vgl. *Ogorek*, Fortgeschrittenenhausarbeit – Öffentliches Recht: Polizeirecht im Auge des Betrachters, 814; vgl. Schenke, Polizei- und Ordnungsrecht, 113.
85 *BVerfG*, Verfassungsrechtliche Überprüfung des Volkszählungsgesetzes 1983, 422.
86 Vgl. *Lang*, Staat, Macht, Eigentum und Freiheit, 108.
87 Vgl. *Andexinger*, Das Spannungsfeld Freiheit versus Sicherheit, 112.
88 *Dalby*, Sicherheitsgesetzgebung unter dem Eindruck von Terror, 97.
89 *BVerfG*, Verfassungsrechtliche Überprüfung des Volkszählungsgesetzes 1983, 422.
90 *Bundestag*, Drucksache 16/545, 3.

Gesetzes nicht hinreichend transparent und differenziert genug ist.[91] Hinter dem hohen Anspruch der detaillierten Gesetzgebung stecken die Bedenken, durch sicherheitsrechtliche Optimierung im Zuge aktueller Bestrebungen der Securitization, Freiheitsrechte übermäßig und ungerechtfertigt zu beschneiden.[92] Es ist ein schmaler „Grat zwischen größtmöglicher Sicherheit bei kleinstmöglicher Beeinträchtigung von Grundrechten".[93] Seit den Anschlägen von 9/11 hat sich die Politik der Inneren Sicherheit verändert. Der Terrorismus wird als Initiator vieler sicherheitspolitischer Maßnahmen gesehen, die im Kampf gegen transnationale Bedrohungen empirisch als unwirksam belegt sind. Paradebeispiel ist die Videoüberwachung.[94] Im Jahre 2011 wurde daher eine Kommission eingerichtet, die „die Sicherheitsarchitektur und -gesetzgebung der vergangenen zehn Jahre einer umfassenden und kritischen Gesamtschau"[95] unterwerfen sollte. In der entsprechenden Pressemitteilung heißt es dazu: „Bei fast 30 neuen Gesetzen seit dem 11. September 2001 war ein distanziertes, sachliches Abwägen zwischen legitimen Sicherheitsinteressen und den verfassungsrechtlich verbrieften Freiheitsrechten kaum noch möglich. (…) Das Austarieren von Freiheit und Sicherheit beginnt gerade im sensiblen Bereich der Terrorismusbekämpfung mit präzisen Analysen zu Tiefe und Streubreite der staatlichen Eingriffe in geschützte Freiheitsrechte der Bürgerinnen und Bürger."[96] Im Zweifel für die Freiheit sagt der Rechtsstaat also aktuell offiziell, aber gleichzeitig ist er bestrebt, das Überwachungsnetz weiter auszubauen. Es darf gesagt werden, dass der Trend ohne Weiteres in Richtung Ausbau privater und staatlicher Videoüberwachung geht.[97] „Geschichte und Philosophie lehren uns, dass alle Absichten, größtmögliche Sicherheit, Wohlfahrt und Glück zu verwirklichen, zum Albtraum werden, wenn ‚echte Freiheit' verloren geht."[98]

Von der staatlichen Videoüberwachung muss im Weiteren noch die private unterschieden werden. Öffentlich zugängliche Räume können auch durch

---

91 Vgl. *BVerfG*, Verfassungswidrige Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten, 833; 846.
92 Vgl. *Dalby*, Sicherheitsgesetzgebung unter dem Eindruck von Terror, 95.
93 *Dalby*, Sicherheitsgesetzgebung unter dem Eindruck von Terror, 95.
94 Vgl. *Fischer/Masala*, Die Politik der Inneren Sicherheit nach 9/11, 1f.
95 Pressemitteilung des *Bundesministeriums der Justiz*, Sicherheitsgesetze auf dem Prüfstand, http://presseservice.pressrelations.de/standard/result_main.cfm?aktion=jour_pm&r=462713, (09.09.2017).
96 Ebd.
97 Vgl. *Groh/Rosch*, Videoüberwachung, 123.
98 *Andexinger*, Das Spannungsfeld Freiheit versus Sicherheit, 114.

nicht öffentliche Stellen überwacht werden. Dazu gehören z. B. Tankstellen oder Banken. Diese Videoüberwachung richtet sich nach § 6 b BDSG.[99] Gemäß dieser Vorschrift dürfen öffentliche und nichtöffentliche Stellen öffentlich zugängliche Räume mit optisch-elektronischen Einrichtungen beobachten. Danach ist die Videoüberwachung auch zweckgebunden und bedarf gem. § 6 b II BDSG der Kenntlichmachung.[100] Für die Zuständigkeitsbereiche öffentlicher Stellen in Ländersache wurden entsprechende Landesdatenschutzgesetze erlassen.[101] § 6 b BDSG wurde im Mai 2001 nachträglich in das Bundesdatenschutzgesetz eingefügt, nachdem man die bisherigen Regelungen nicht mehr für ausreichend erachtete. Denn zuvor war das Recht am eigenen Bild lediglich strafrechtlich über das Kunsturhebergesetz (KUG) und als subjektives Recht über die Schadenersatzvorschriften des Bürgerlichen Gesetzbuches (BGB) geschützt. Den Anstoß zum Umdenken und Handeln gaben final die Europäischen Datenschutzrichtlinien von 1995, die schließlich in nationales Recht umgesetzt werden müssen. Auf der Ebene des europäischen Rechts steht Art. 8 EMRK für das Recht auf Privatheit und ist damit Dreh- und Angelpunkt der rechtsstaatlichen Debatte.[102]

Die Videoüberwachung von Privatgrundstücken durch Privatpersonen ist grundsätzlich zulässig, sofern dadurch keine Persönlichkeitsrechte Dritter betroffen sind und sich die Aufnahmen auf das Eigentum beschränken.[103]

2.3 Zum technischen Standard und der DIN

Die Kamera-Hardware und die technischen Möglichkeiten von Videoüberwachungsanlagen haben in der vergangenen Zeit einen außergewöhnlichen Fortschritt erfahren.[104] Aus polizeilicher Sicht wird die Ermittlungstätigkeit bedau-

---

[99] Vgl. *Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BFDI)*, Videoüberwachung, https://www.bfdi.bund.de/DE/Datenschutz/Themen/Technische_Anwendungen/TechnischeAnwendungenArtikel/Videoueberwachung.html, (10.09.2017).

[100] Die Speicherungsfrist wird bewusst nicht weiter angesprochen, da sie ein eigener großer Themenkomplex ist, der das eigentliche Thema der Arbeit nur peripher tangiert.

[101] Vgl. *Kühling et al.*, Datenschutzrecht, 229f. Die länderspezifischen Rechtsgrundlagen sind § 20 a LDSG (Baden-Württemberg), Art. 21 a BayDSG, § 31 b BlnDSG, § 33 c BbGDSG, § 20 b BremDSG, § 30 HmbDSG, § 37 DSG M-V, § 25 a NDSG, § 29 b DSG NRW, § 34 LDSG (Rheinlandpfalz), § 34 SDSG, § 33 SächsDSG, § 30 DSG LSA, § 20 LDSG S-H, § 25 a ThürDSG. Hessen hat bisher keine ausdrückliche Regelung für die Videoüberwachung öffentlich zugänglicher Räume im HDSG getroffen.

[102] Vgl. *Weichert*, Private Videoüberwachung und Datenschutzrecht, https://www.datenschutzzentrum.de/video/videpriv.htm, (17.09.2017).

[103] Vgl. *BGH*, Urteil vom 16.03.2010, Az. VI ZR 176/09, Rn. 5.

[104] Vgl. *Blindenbacher/Müller*, Intelligente Videoüberwachung im öffentlichen Raum, 30.

erlicherweise häufig durch die mangelhafte Bildqualität von Untersuchungsmaterial aus Videoüberwachungsanlagen begrenzt.[105] Diese Aspekte sind auf den ersten Blick schwer miteinander vereinbar. Einerseits wird auf dem Gebiet der Videoüberwachung, beziehungsweise Kameratechnik, hoch- und weiterentwickelt, andererseits bleibt das gelieferte Bildmaterial qualitativ erstaunlich verbesserungswürdig.

Es lohnt sich der Blick auf die Vorgaben der deutschen Normung von Videoüberwachungsanlagen für Sicherheitsanwendungen, die DIN EN 62676-4 (VDE 0830-71-4):2016-07. Es handelt sich dabei um eine aktuelle Richtlinie aus 2016 für Videoüberwachungsanlagen, um „die Erfüllung ihrer Anforderungen an Funktion und Betriebsverhalten sicher[zu]stellen."[106] Die Norm definiert, was detektieren, identifizieren, überprüfen und erkennen im Zusammenhang mit Videoüberwachung bedeutet und auch, welche technischen Voraussetzungen dafür mindestens gegeben sein müssen.

An dieser Stelle sollen besonders das Identifizieren und das Überprüfen im Sinne der Richtlinie hervorgehoben werden. Bei „identifizieren" steht erläuternd: „festgelegte funktionelle Bestimmung einer Kamera zur Ermöglichung der **zweifelsfreien Identifizierung** eines Individuums".[107] Zum „Überprüfen" liest man: „festgelegte funktionelle Bestimmung einer Kamera zur Befähigung der Bedienperson zum Erhalt von Informationen bezüglich eines Objektes. Anmerkung 1 zum Begriff: Ein Beispiel für ein Objekt kann einen Text oder ein Logo auf Kleidungsstücken einschließen".[108]

Die Norm gibt vor, dass bei der Auflösung für die Identifizierung eines Ziels in einem Bild eine Pixelgröße von 4 mm ausreichend ist. Für die Überprüfung wird mindestens eine Größe von 1 mm/Pixel gefordert.[109] Das ist nicht annähernd das, was technisch im Jahr 2016 im Bereich der Bildauflösung möglich ist. Im Vergleich dazu: Das neue iPhone X hat eine 12 Megapixel Kamera integriert. Diese hat eine Auflösung von 4048x3040 Pixel. Das Mobiltelefon kann entsprechend hochaufgelöste Fotos schießen, bei denen ein Pixel eine Größe von ca. 0,12 mm hat. Selbst ein Standbild mit 8 Megapixeln, während einer 4K

---

[105] Vgl. *Humer/Lederer*, Von der konventionellen zur intelligenten Videoüberwachung – Chancen und Risiken für Polizei und Gesellschaft, 38.
[106] *DKE*, DIN EN 62676-4 (VDE 0830-71-4):2016-07, 8.
[107] *DKE*, DIN EN 62676-4 (VDE 0830-71-4):2016-07, 11. Hervorhebung durch den Autor.
[108] *DKE*, DIN EN 62676-4 (VDE 0830-71-4):2016-07, 11.
[109] *DKE*, DIN EN 62676-4 (VDE 0830-71-4):2016-07, 25.

Videoaufnahme mit dem iPhone X, ist besser als der derzeitig geforderte Mindeststandard der Bildauflösung bei Videoüberwachungsanlagen zur Sicherheitsproduktion.[110] Zur Veranschaulichung, was diese Worte in Bildern bedeuten, siehe *Abbildung 1*.

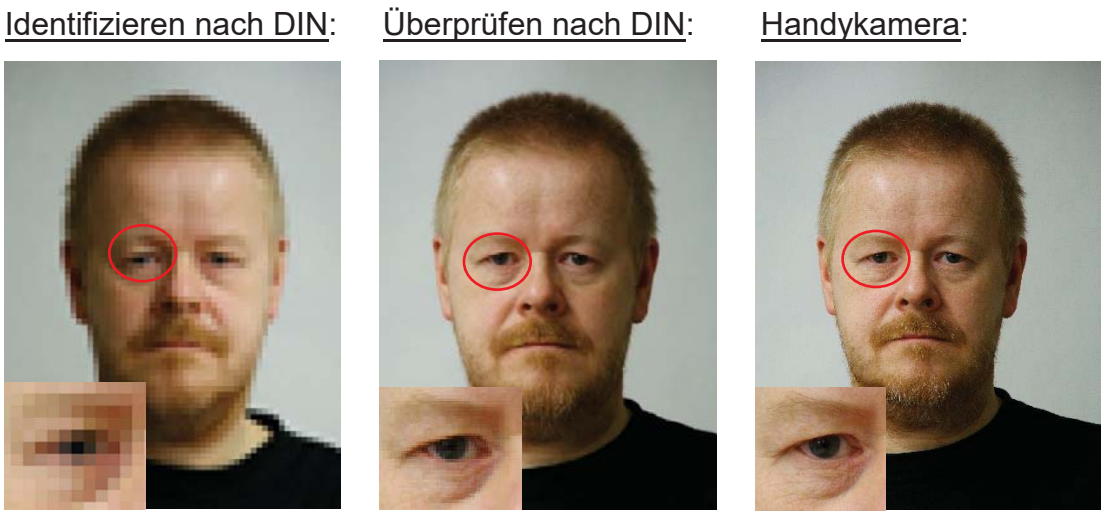

Abbildung 1: Verbildlichung der Auflösungen von 4 mm/Pixel bis 0,12 mm/Pixel[111]

Daraus folgt, dass das „Identifizieren" im Sinne der DIN sinngemäß eher einem Feststellen der Abbildung eines Menschen, keinesfalls aber einer zweifelsfreien Identifikation gleichkommt.

Ein Missverständnis oder eine ungünstige Wortwahl sind ausgeschlossen, denn die DIN definiert das reine Feststellen der Abbildung eines Menschen im Bild als „erkennen" und schreibt dafür 8 mm/Pixel vor, das heißt, jeder einzelne Pixel ist dann sogar doppelt so groß wie im ersten Bild.[112] Würde man dagegen den Mindeststandard der Überprüfung auch für die Identifizierung anlegen, erscheint eine zweifelsfreie Identifikation schon wahrscheinlicher. Davon mal abgesehen, dass rein technisch weitaus mehr möglich ist.

2.4 Zusammenfassung wesentlicher Kritikpunkte

Abschließend lassen sich die folgenden wesentlichen Kritikpunkte zur Videoüberwachung zusammenfassen. Der Einsatz von Videotechnik wird zur Sicherheitsproduktion instrumentalisiert und führt dadurch zu Diskriminierung

[110] Vgl. zur Technik des iPhone X, https://www.apple.com/de/iphone-x/specs/, (23.09.2017).
[111] Darstellung von *Frank Kürpiers*, Dipl.-Ing., HLKA, SG 643.
[112] Vgl. *DKE*, DIN EN 62676-4 (VDE 0830-71-4):2016-07, 12.

und Verdrängung von Randgruppen aus den überwachten Gebieten. Dies produziert wiederum soziale Ungleichheit und auch soziale Ungerechtigkeit.
Es gibt weder unbestreitbare Erfolgsmeldungen zum positiven Einfluss auf die Strafverfolgung, noch lassen sich Werte zum Präventionsgehalt messen. Weiterhin wurde festgestellt, dass sich einerseits lediglich ein Verdrängungseffekt abzeichnet und andererseits kein erheblicher Einfluss auf die Motivation des Täters genommen werden kann.
Das subjektive Sicherheitsgefühl der Bevölkerung wird bei differenzierter Betrachtung nur bedingt gestärkt. Gleichzeitig darf die hohe Akzeptanz der Technik keine Grundlage für die Legitimation ihres Einsatzes sein. Die Videoüberwachung ist kein Allheilmittel im Kampf gegen die Kriminalität, sondern kann lediglich ermittlungsunterstützend eingesetzt werden. Sie schafft durch ihre Installation unsichere Gebiete und führt somit zur Stigmatisierung von Räumen. Aus juristischer Sicht wird bemängelt, dass die Videoüberwachung potenziell rechtsstaatliche Prinzipien wie die Unschuldsvermutung verdrängt und eine hohe Anzahl unbeteiligter unter Generalverdacht gestellt werden. Die gesetzlichen Regelungen zum Einsatz und Zweck der Videoüberwachung werfen kompetenzrechtliche Fragen auf. Materiellrechtlich kollidiert die Maßnahme mit mehreren Grundrechten, vor allem aber mit dem Recht auf informationelle Selbstbestimmung, weshalb eine strenge Abwägung der Verhältnismäßigkeit verpflichtend sein sollte. Die Videoüberwachung kann zurück zum Überwachungsstaat führen und die demokratischen Freiheitsrechte der Bürger massiv beschneiden. Aus kriminalistischer Sicht wird, trotz besserer technischer Möglichkeiten, die schlechte Bildqualität der Aufnahmen moniert und somit die Videoüberwachung als Sicherheitsmaßnahme in ihre Schranken gewiesen.

3 Die Gesichtserkennung

Videoüberwachung und Gesichtserkennung sind auf dem Gebiet der Strafverfolgung(-svorsorge) inzwischen eng verknüpft. Bei dieser Verbindung spricht man von intelligenter Videoüberwachung. „Intelligente Videoüberwachung ist längst keine Utopie mehr. Kameras sind inzwischen nicht nur digital, sie werden zunehmend „intelligent“. Ging es früher meist um das Beobachten an sich, laufen heutzutage immer öfter Systeme im Hintergrund mit, die live oder zeit-

nah Analysen durchführen, beispielsweise im polizeilichen Bereich zu Fahndungszwecken. (…) Die Zeiten des bloßen Schauens und Speicherns sind vorbei.“[113] Die Analysen basieren auf Algorithmen und Mustererkennung. Den Algorithmen und Mustern, liegt die Biometrik zugrunde.[114] „Die Biometrik ist die Disziplin der Vermessung quantitativer Identifikationsmerkmale von Individuen. Diese Merkmale dienen, als digitales Referenzmuster abgespeichert, entweder der Authentifikation oder der Identifikation“[115]. Ungeachtet ihrer Verbindung zur Videoüberwachung, können das Prinzip der Gesichtserkennung und die Biometrie auch im Ermittlungsverfahren Anwendung finden.

3.1 Kriminalistische Relevanz

Die Maßnahmen der Gesichtserkennung gehören mittlerweile zu den wichtigsten biometrischen Identifizierungsmethoden im Ermittlungsverfahren. Sie funktionieren weitestgehend ohne die Kooperationsbereitschaft des Beschuldigten.[116] In der Kriminalistik müssen zwei Arten der Gesichtserkennung differenziert werden. Man muss die computergestützte Gesichtserkennung (GES) von der Ermittlungshilfe des Lichtbildvergleiches, durch anthropologische bzw. morphologische Begutachtung des Gesichts, abgrenzen.[117] Beide Methoden haben mit Muster-, Merkmals- und Wiedererkennung zu tun und gehören zu den kriminaltechnischen Untersuchungsmöglichkeiten im Ermittlungsverfahren.[118]

Die Gesichtserkennung und der Lichtbildvergleich zählen zu den Personenidentifizierungsverfahren, da sie Personen anhand ihrer individuellen und charakteristischen körperlichen Merkmale erkennen, sie gehören aber nicht zu den Wiedererkennungsverfahren und Wiedererkennungsmaßnahmen im klassischen Sinne.[119] Im Wiedererkennungsverfahren soll meistens ein Zeuge einen inzwischen bekannten Beschuldigten zum Beispiel per Gegenüberstellung oder Wahllichtbildvorlage nach seiner getätigten Personenbeschreibung zu einem späteren Zeitpunkt der Ermittlungen re-identifizieren.[120] Ähnliches

[113] *Humer/Lederer*, Von der konventionellen zur intelligenten Videoüberwachung – Chancen und Risiken für Polizei und Gesellschaft, 36.
[114] Vgl. *Ranftl*, Digitale Gesichtserkennung, 4.
[115] *Hompel/Büchter/Franzke*, Identifikationssysteme und Automatisierung, 11.
[116] Vgl. *Hengfoss et al.*, Herausforderung bei der Gesichtserkennung, 699.
[117] Vgl. *Huckenbeck et al.*, Identifikation lebender Personen anhand von Lichtbildern des Gesichts, 5.
[118] Vgl. *Averdiek-Gröner/ Frings*, Standardmaßnahmen im Ermittlungsverfahren, 131f.
[119] Vgl. *Wirth*, Kriminalistik-Lexikon, 425.
[120] Vgl. *Clages/Ackermann*, Der rote Faden, 247ff.

gilt für den Lichtbildvergleich, wo das Bild eines unbekannten Täters mit dem Lichtbild eines Verdächtigen abgeglichen wird. Bei der Gesichtserkennung liegt ein Lichtbild des Täters vor, welches mit der polizeilichen Datenbank abgeglichen werden soll, um überhaupt erst einen Tatverdächtigen zu ermitteln.[121] Es handelt sich hierbei jedoch rein um den Gebrauch und die Auswertung von Sachbeweisen, wohingegen ein Zeuge und seine Aussage einen Personalbeweis darstellen.[122]

Der Ursprung der Basis dieser kriminalistischen Methoden zur Gesichtserkennung liegt im 19. Jahrhundert. Dort sind die Anfänge der heutigen erkennungsdienstlichen Behandlung, in Form von Ablichtungen und Personenvermessung zu notieren. Straftäter wurden zunächst bildlich festgehalten und später nach ihren Körpermaßen und ihrem Knochenbau über Messkarten katalogisiert.[123] Die Daguerreotypie, benannt nach Louis Jacques Daguerre, ermöglichte es 1838 erstmalig Fotografien herzustellen.[124] Die Bestimmung der Körpermaße zur Identifizierung einer Person, die Anthropometrie, geht, ebenfalls Mitte des 19. Jahrhunderts, auf Adolphe Quetelet zurück. Quetelet glaubte, dass sich Teile des menschlichen Körpers ab einem gewissen Alter nicht mehr wesentlich verändern und dass die Kombination der einzelnen Maße so individuell sei, dass es keine zwei Menschen mit denselben gibt. Davon ausgehend erarbeitete Alphonse Bertillon die Bertillonage, ein Körpermessverfahren bei dem immer die gleichen Maße erhoben wurden, zum Beispiel Länge und Breite der Ohren. Lichtbilder gehörten auch zur Bertillonage. Dieses Verfahren wurde, teilweise nur ähnlich, zur Registrierung von Straftätern in vielen Ländern bei der Polizei eingeführt und findet sich noch heute in der erkennungsdienstlichen Behandlung wieder.[125] Allerdings beschränkt sich die Beschreibung gegenwärtig auf die Körpergröße, sowie einzelne besondere Merkmale und geschlossene Angaben zu bestimmten Körperregionen.[126] Insbesondere die Personenaufnahmen nach bestimmten Positionen auf dem Bertillon-Stuhl ähnelten damals schon den Täterlichtbildern der Neuzeit.[127]

---

[121] Vgl. *Averdiek-Gröner/Frings*, Standardmaßnahmen im Ermittlungsverfahren, 132.
[122] Vgl. *Clages/Ackermann*, Der rote Faden, 48.
[123] Vgl. *Kube*, Beweisverfahren und Kriminalistik in Deutschland, 133; 136.
[124] Vgl. *Kube*, Beweisverfahren und Kriminalistik in Deutschland, 133.
[125] Vgl. *Wirth*, Kriminalistik-Lexikon, 34f.; vgl. *Thiel*, Identifizierung von Personen, 98.
[126] Vgl. *Thiel*, Identifizierung von Tätern, 98.
[127] Vgl. *Wirth*, Kriminalistik-Lexikon, 75.

Bereits 1901 löste in England die Daktyloskopie die Bertillonage wieder ab. In Deutschland führte man das daktyloskopische Identifizierungsverfahren wenige Jahre später ebenfalls ein. In Berlin nutzte man Bertillonage und Daktyloskopie zunächst nebeneinander, bis man ab 1914 nur noch ausschließlich mit Fingerabdrücken arbeitete.[128] Der Diebstahl der „Mona Lisa“ aus dem Louvre im selben Jahr wurde zum Präzedenzfall und initiierte die Einführung der Daktyloskopie in Frankreich. Der Täter hinterließ Fingerabdrücke am Tatort und hätte dadurch leicht ermittelt werden können, wohingegen sich die Bertillonage damals zur Identifizierung des Täters als ungeeignet erwies.[129]
Ihr Revival erfährt die Biometrie in abgewandelter sowie moderner Form in den bereits erwähnten Methoden des Lichtbildvergleiches und der computergestützten Gesichtserkennung. Für diese Verfahren sind die Vermessungen des Gesichtes und seiner Merkmale essentiell. Im Jahr 2008 wurde beim Bundeskriminalamt die Software zur Gesichtserkennung implementiert. Auch das HLKA führt mit dieser Software ihre Untersuchungen der GES- Recherche durch. Etwa seit dieser Zeit gibt es dort auch die Lichtbildvergleiche durch besonders geschultes Personal.[130]

3.2 Computergestützte Gesichtserkennung (GES)

Polizisten können, wenn sie im Zuge von Ermittlungen auf ein Lichtbild des noch unbekannten Tatverdächtigen stoßen, in Hessen beim Landeskriminalamt einen Untersuchungsantrag auf Gesichtserkennungsrecherche stellen. Bei der Recherche mit der Gesichtserkennungssoftware, werden die Bilder der unbekannten Personen aus den Ermittlungsverfahren mit einer polizeiinternen Datenbank abgeglichen. In dieser recherchefähigen Referenzdatenbank befinden sich die Lichtbilder erkennungsdienstlicher Behandlungen.[131]
Der Hersteller Cognitec wirbt auf seiner Homepage damit, dass Strafverfolgungsbehörden dank der Gesichtserkennungssoftware FaceVACS-DBScan auf oben beschriebene Art und Weise Straftaten aufklären und Täter identifizieren können. Man kann dort sogar sehen, wie eine solche Benutzeroberfläche aussieht und wie das System praktisch funktioniert, siehe *Abbildung 2*.[132]

---

[128] Vgl. *Kube*, Beweisverfahren und Kriminalistik in Deutschland, 139.
[129] Vgl. *Kube*, Beweisverfahren und Kriminalistik in Deutschland, 139.
[130] Vgl. *Averdiek-Gröner/Frings*, Standardmaßnahmen im Ermittlungsverfahren, 131f.
[131] Vgl. *Averdiek-Gröner/Frings*, Standardmaßnahmen im Ermittlungsverfahren, 132.
[132] Vgl. *Cognitec*, http://www.cognitec.com/facevacs-dbscan.html, (07.10.2017).

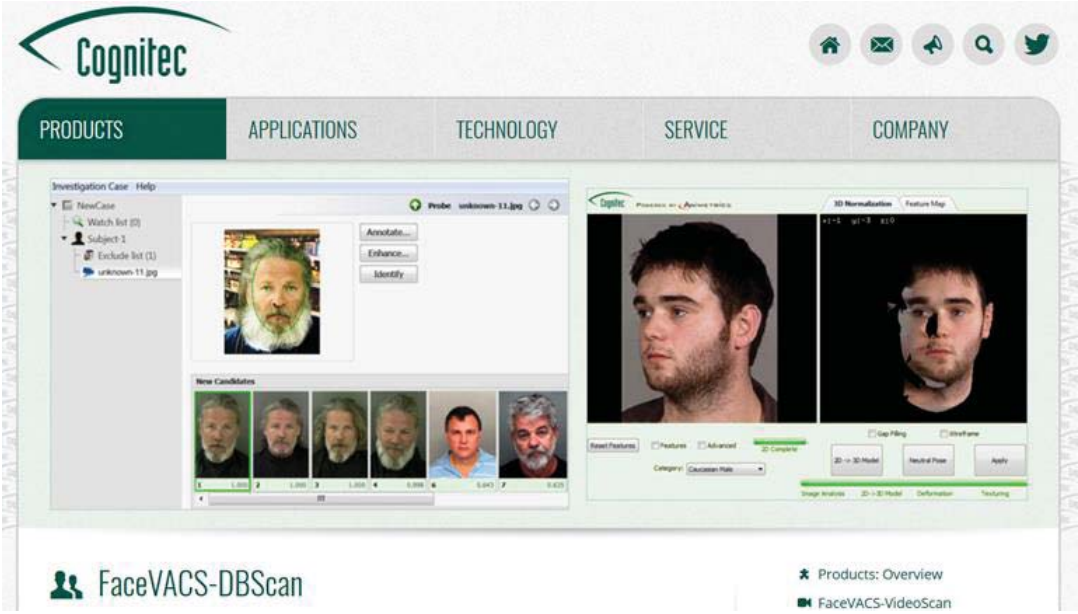

Abbildung 2: Screenshot der Benutzeroberfläche einer GES-Software

Theoretisch und vom Prinzip läuft die Gesichtserkennung genauso ab, wie bei der intelligenten Videoüberwachung, nur nicht automatisch in Echtzeit, sondern händisch initiiert. Es handelt sich um eine Art Wiedererkennungsverfahren, wenngleich nicht im klassischen Sinne. Anstelle eines Zeugen erkennt die Technik eine Person aus Referenzmaterial.[133] Die Software gibt, je nach Einstellung, 200 Vorschläge mit numerischen Wahrscheinlichkeitsangaben zur Übereinstimmung der Personen an. Jeder Treffer wird durch einen sachverständigen Beamten angesehen. Nach der Überprüfung der Ergebnisse der Software, wird von dem Sachverständigen ein Gutachten für den Sachbearbeiter verfasst.[134] Bei der Gesichtserkennung handelt es sich insofern um ein nicht kooperatives Verfahren, da die Bilder ohne Zutun der betroffenen Person aufgenommen wurden und ihre biometrischen Merkmale auch ohne ihr Mitwirken abgeglichen werden können.[135] Bei diesen Recherchen darf es sich nicht um beliebige Lichtbilder des Tatverdächtigen handeln. Durch die Arbeitsweise und Programmierung der Software müssen hohe Anforderungen an das Bildmaterial gestellt werden. Bildmaterial ist am besten geeignet, wenn es ein Gesicht frontal zeigt, wie bei den biometrischen Reisepässen und eben der erkennungsdienstlichen Behandlung. Diese Position und Haltung des Kopfes ist

[133] Vgl. *Pretzel*, Warum die Gesichtserkennung als Fahndungshilfe vorerst nicht einsatzfähig ist, 42.
[134] Vgl. *Averdiek-Gröner/Frings*, Standardmaßnahmen im Ermittlungsverfahren, 132.
[135] Vgl. *Pretzel*, Warum die Gesichtserkennung als Fahndungshilfe vorerst nicht einsatzfähig ist, 42.

zur Identifizierung einer Person durch ein computergestütztes Gesichtserkennungsverfahren optimal.[136] Schnell wird deutlich, dass die Gesichtserkennung Grenzen hat. Videoüberwachung und Biometrie sind in ihrer Kombination sehr täuschungsanfällig. Ein gutes Beispiel dafür findet sich 2010 in Amerika, wo Überwachungskameras einen dunkelhäutigen Bankräuber mit Sonnenbrille aufzeichneten. Dank der guten Qualität der Aufnahmen waren einzelne Gesichtsmerkmale zu erkennen. Es stellte sich im Laufe der Ermittlungen jedoch heraus, dass der Täter eine helle Hautfarbe und für die Überfälle eine qualitativ hochwertige dunkle Gesichtsmaske getragen hatte. Es zeigt sich dadurch ebenfalls, dass die Gesichtserkennung gegen Maskierung, und auch gegen Vermummung durch Kleidungsstücke oder Accessoires, machtlos ist. Selbst eine Gesichtsbemalung stellt die Analysesoftware vor Probleme. Sie kann weiterhin nur Kopfneigungen bis etwa 15 Grad eruieren und zeigt sich somit recht unflexibel.[137] Auch *Hengfoss et. al.* konstatieren, dass Gesichter nicht invariant sind und dauernden Veränderungsprozessen unterliegen. Selbst nach jahrzehntelanger Forschung auf dem Gebiet der Gesichtserkennung sind Tatsachen wie Alterungsprozesse, Beleuchtung, Gesichtsausdrücke und -drehungen immer noch Herausforderungen für die Analysesysteme geblieben. Problematisch sei im Bereich der Gesichtsidentifikation zudem nach wie vor die Unterscheidung eineiiger Zwillinge.[138] Die folgende Frage ist, wie funktioniert die Mustererkennung, wenn sie funktioniert? Die Mustererkennung ist, gleich in Bezug auf welches Wissenschaftsgebiet, immer die „Suche nach Strukturen in Daten“.[139] Die Analysesoftware der Polizei bedient sich dabei spezieller Algorithmen, die das Bildmaterial aus einem Ermittlungsverfahren mit bekannten Mustern des Bildmaterials aus der Referenzdatenbank abgleicht.[140] Ein Algorithmus ist ein schematischer, sich wiederholender Rechenvorgang.[141] Grob gesagt, kann die Software dabei das Gesicht in verschiedene Zonen untergliedern, wie die Augenpartie oder den Mund. In den Bereichen werden dann verschiedene Größen, Längen und Lagen zueinander gemessen, bestimmt und

[136] Vgl. *Thiel*, Identifizierung von Personen, 132.
[137] Vgl. *Nouak*, Grenzen der Gesichtserkennung, 14f.
[138] Vgl. *Hengfoss et al.*, Herausforderungen bei der Gesichtserkennung, 699.
[139] *Held*, Intelligente Videoüberwachung, 23.
[140] Vgl. ähnlich zur algorithmischen Analyse auch *Held*, Intelligente Videoüberwachung, 50.
[141] Vgl. *Scholze-Stubenrecht*, Duden, 124.

zu einer Schablone verformelt. Der sich anschließende Abgleich mit den gespeicherten Schablonen aus der Datenbank wird in Fachkreisen Matching genannt. Die meisten Analysen bestehen aus der Kombination eines Abgleiches Merkmal basierter einzelner Schablonen von charakteristischen Gesichtsbereichen und holistischen Ansätzen, bei denen das ganze Gesicht zum Matching verwendet wird.[142]

3.3 Lichtbildvergleiche

„Der Lichtbildvergleich basiert auf der Grundlage, dass die anatomische Individualität des Gesichts und des Kopfes dem Menschen eine Einmaligkeit verleiht.“[143] Die Individualität basiert dabei sowohl auf der Genetik einer Person als auch auf den Umwelteinflüssen, derer sie ausgesetzt ist. Somit ist jeder Mensch von anderen optisch unterscheidbar.

Der Lichtbildvergleich kommt vor allem immer dann im Ermittlungsverfahren in Betracht, wenn der Täter keine Spuren am Tatort hinterlassen hat, aber Bildmaterial von ihm gefertigt wurde. Über den Lichtbildvergleich kann dann der Nachweis oder ein Ausschluss von Personenidentität geführt werden.[144] Wichtig zu erwähnen ist, dass es sich hierbei im Wesentlichen um die morphologische Begutachtung des Gesichts handelt und nicht des ganzen Körpers. Der Lichtbildvergleich ist allgemeinhin und bei Gericht als anthropologisches Gutachten bekannt, obwohl anthropos theoretisch und wörtlich die Begutachtung des Körpers, also des gesamten Menschen, bedeuten würde.[145]

Der Lichtbildvergleich ist ein direkter Bild-Bild-Vergleich. Das bedeutet, das Bildmaterial vom Tatort muss mit einem Vergleichsbild des Tatverdächtigen abgeglichen werden.[146] Als Untersuchungsmaterial kommen zum Beispiel Fotos und Videos aus Überwachungskameras, von Speicherkarten, Festplatten, Handys oder aus Sozialen Netzwerken in Betracht. Wichtig im Zusammenhang mit Bildmaterial aus online Profilen und dem Privatbereich ist die Überprüfung der Echtheit und der Ausschluss von Manipulation des Bildes durch

---

[142] Vgl. *Tomii/Scheer*, https://www2.informatik.hu-berlin.de/Forschung_Lehre/algorithmenII/Lehre/SS2004/Biometrie/05Gesicht/gesichtserkennung.pdf#page=4&zoom=auto,-82,656, (07.10.2017).

[143] Vgl. *Averdiek-Gröner/Frings*, Standardmaßnahmen im Ermittlungsverfahren, 132.

[144] Vgl. *Huckenbeck et al.*, Identifikation lebender Personen anhand von Lichtbildern des Gesichts, 5.

[145] Vgl. *Gabriel et al.*, Über die Fragwürdigkeit der Berechnung einer Identitätswahrscheinlichkeit in anthropologischen Gutachten, 346.

[146] Vgl. *Averdiek-Gröner/Frings*, Standardmaßnahmen im Ermittlungsverfahren, 132.

Bildbearbeitung. Das Bild muss ein originales Abbild der zu untersuchenden Person sein.[147]

Die Aufnahmen, mit denen das Untersuchungsmaterial abgeglichen werden soll, sollten eine ähnliche Perspektive haben. Bilder aus erkennungsdienstlichen Behandlungen eignen sich prinzipiell gut, da sie mit unterschiedlichen Blickrichtungen und in sehr guter Auflösung vorliegen. Ähnliches gilt für Passbilder, allerdings sind diese auf Frontalaufnahmen begrenzt und daher nur bedingt geeignet.[148] Wie auch bei der Gesichtserkennung, werden beim Lichtbildvergleich hohe Anforderungen an das Bildmaterial gestellt. Das Prädikat der Beurteilung hängt maßgeblich von der Qualität der Bilder ab. Experten differenzieren zwischen internen und externen Störfaktoren. Interne Störfaktoren sind Mängel, die von der abgelichteten Person ausgehen. Dazu gehören Aspekte wie Gewichtsverlust oder Gewichtszunahme, Alterungsprozesse, Maskierung, Krankheit, Gesichtsgrimassen oder -operationen sowie Gesichtsaccessoires und Bewegungsunschärfe. Externe Störfaktoren sind hingegen technisch bzw. situationsbedingt. Dazu zählen Bildkompression, Bildinterpolation, Unschärfe, zu kleine Abbildungsgrößen aufgrund eines ungeeigneten Kamerastandortes, perspektivische Verzerrungen oder schlechte Lichtverhältnisse. Externe Störfaktoren lassen sich geringfügig durch digitale Bildbearbeitung reduzieren, eine erhebliche Verbesserung oder eine Darstellung verborgener Informationen ist jedoch nachträglich nicht möglich.[149]

Die Bilder werden in einem ersten Schritt durch einen Sachverständiger in Augenschein genommen und dahingehend untersucht, ob objektiv individuelle Merkmale für eine Auswertung erkennbar sind. Es geht dabei um den Gesamteindruck der Merkmalsbereiche, der Proportionen und der Bildqualität. Bei der Beurteilung des Bildmaterials als ungenügend, endet die Auswertung an diesem Punkt.[150]

Die Frage im weiteren Verlauf ist, wie der Vergleich bei guten Voraussetzungen und geeignetem Material funktioniert. In einem „Detailvergleich werden die Merkmalsbereiche des Gesichts in möglichst fein unterteilten Einzelmerkmalen betrachtet und beschrieben“.[151] Zu den Merkmalsbereichen gehören die

---

147 Vgl. *Huckenbeck et al.*, Identifikation lebender Personen anhand von Lichtbildern des Gesichts, 6.
148 Vgl. *Huckenbeck et al.*, Identifikation lebender Personen anhand von Lichtbildern des Gesichts, 8.
149 Vgl. *Huckenbeck et al.*, Identifikation lebender Personen anhand von Lichtbildern des Gesichts, 6.
150 Vgl. *Huckenbeck et al.*, Identifikation lebender Personen anhand von Lichtbildern des Gesichts, 6f.
151 *Huckenbeck et al.*, Identifikation lebender Personen anhand von Lichtbildern des Gesichts, 6.

Gesichtsform ebenso wie die Augenregion, die Mundpartie, der Kiefer, die Ohren, der Hals und einige mehr. Jeder dieser Bereiche kann in zahlreiche Einzelmerkmale und die einzelnen Merkmale wiederum in Submerkmale ausdifferenziert werden.[152] „Im Merkmalskomplex der Augenregion sind das beispielsweise Augenbrauen, Oberlidraum, Augenabstand, Lidachsenstellung, Unterlid. Die Beschreibung sollte so genau wie möglich sein und im Falle der Augenbrauen als Submerkmale beispielsweise auch Breite, Höhe, Dichte, Länge, Form, Verlauf, Brauenkopfabstand umfassen.“[153] Jedes erkennbare Merkmal aus dem Untersuchungsmaterial wird im Vergleichsbild abgeglichen und gegenübergestellt. Alle Abweichungen und Übereinstimmungen werden vom Experten notiert und bewertet. Es ist seine Aufgabe zu beurteilen, ob eine Abweichung durch Störfaktoren erklärbar ist, oder zum Identitätsausschluss führt. Hier gilt der Grundsatz in dubio pro reo. Diese Technik des Merkmalvergleichs nennt sich Basismethodik.[154]

Entscheidend für die Vergabe des endgültigen Prädikates ist die Anzahl der beschreibbaren Merkmale. Je mehr Merkmale übereinstimmen, desto größer ist die Gewissheit, dass es sich um Personengleichheit handelt und desto höher wird das Prädikat des Gutachters ausfallen. Dabei wird jeweils auch berücksichtigt, dass Merkmale unterschiedlich gewichtig sein können.[155] „Es gibt Merkmale, die vielen Menschen eigen sind, es gibt andererseits Merkmale, die ausgesprochen individualtypisch sind – Narben, Warzen, Muttermale etc. – und deshalb bei einer vergleichenden morphologischen Analyse stärker gewichtet werden dürfen“[156]. Andersherum kann so schon ein einziges abweichendes Merkmal zum Ausschluss der Personengleichheit führen. Finden sich sowohl übereinstimmende als auch abweichende Merkmal in höherer Anzahl, so kann dies ein Hinweis auf Verwandtschaft sein.[157]

Der Lichtbildvergleich ist eine deskriptive Ermittlungsmethode. Das Prädikat, welches am Ende der Begutachtung zu vergeben ist, ist daher bewusst ein sprachliches. Für eine numerische oder mathematische Wahrscheinlichkeitsangabe über eine Identität der betrachteten Personen, müsste es empirisch

[152] Vgl. *Huckenbeck et al.*, Identifikation lebender Personen anhand von Lichtbildern des Gesichts, 8.
[153] *Huckenbeck et al.*, Identifikation lebender Personen anhand von Lichtbildern des Gesichts, 8.
[154] Vgl. *Huckenbeck et al.*, Identifikation lebender Personen anhand von Lichtbildern des Gesichts, 8.
[155] Vgl. *Huckenbeck et al.*, Identifikation lebender Personen anhand von Lichtbildern des Gesichts, 7.
[156] *Huckenbeck et al.*, Identifikation lebender Personen anhand von Lichtbildern des Gesichts, 7.
[157] Vgl. *Huckenbeck et al.*, Identifikation lebender Personen anhand von Lichtbildern des Gesichts, 7.

gesicherte Zahlen zur Häufigkeitsverteilung morphologischer Erkennungsmerkmale geben.[158]

In einem Aufsatz von *Gabriel et al.* stellt *Kürpiers* sogar dar, dass sich bisher bekannte und ermittelte Auftretenswahrscheinlichkeiten in Prozent aus drei verschiedenen veröffentlichten Studien nicht signifikant von beliebig gewürfelten Identitätswahrscheinlichkeiten unterscheiden.[159] Zurzeit gibt es daher weder entsprechende zuverlässige Datenbanken noch valide Berechnungen unter Einbezug der gesamten Weltbevölkerung. Aktuell werden Häufigkeiten daher nach Erfahrungswerten beurteilt. Sachverständige kategorisieren häufige Merkmale als wenig individualtypisch. Merkmale, die weniger oft auftreten sind mäßig individualtypisch, seltene Merkmale sind individualtypisch und sehr seltene nennt man Individualmerkmale. Als Ergebnis kommen in polizeilich entstandenen Gutachten elf verbale Prädikatsstufen in Betracht. Lässt ein zugrunde liegendes Bildmaterial nur tendenzielle Aussagen zu, stehen den Gutachtern differenziertere Prädikate zur Verfügung, als wenn eine Bewertung höherrangig ist. Die Prädikate werden außerdem in positiv und negativ unterschieden. Spricht ein Vergleich dafür, dass es sich bei den abgeglichenen Personen um ein und dieselbe handelt, dann können, je nach Ausprägung, folgende Aussagen durch den Experten getroffen werden: (1) Es handelt sich mit an Sicherheit grenzender Wahrscheinlichkeit, (2) mit hoher Wahrscheinlichkeit oder (3) wahrscheinlich um dieselbe Person. Weiterhin gibt es die Prädikate (4) es deutet daraufhin und (5) es kann nicht ausgeschlossen werden, dass es sich um ein und dieselbe Person handelt. Dieselben fünf Prädikate können auch verwendet werden, um auszudrücken, dass es sich nicht um ein und dieselbe Person handelt. Das elfte mögliche Urteil lautet, es kann weder bestätigt, noch ausgeschlossen werden, dass es sich um ein und dieselbe Person handelt. Es ist das schwächste Prädikat, weil es keine wertende Tendenz besitzt.[160] Dennoch ist dieses Prädikat im Ermittlungsverfahren nicht unbrauchbar, denn die freie Beweiswürdigung liegt gem. § 261 StPO beim Richter. Dieser wird nach Betrachtung aller Beweise zu einem Urteil darüber kommen, ob er den Angeklagten für schuldig hält oder nicht.

---

[158] Vgl. *de Vries*, Einführung in die Kriminalistik für die Strafrechtspraxis, 82.

[159] Vgl. *Gabriel et al.*, Über die Fragwürdigkeit der Berechnung einer Identitätswahrscheinlichkeit in anthropologischen Gutachten, 349.

[160] Vgl. *Huckenbeck et al.*, Identifikation lebender Personen anhand von Lichtbildern des Gesichts, 9.

3.4 Rechtliche Einordnung

Für computergestützte Gesichtserkennung im Anwendungsbereich intelligenter Videoüberwachung, finden die bereits unter Punkt 2.2 diskutierten Grundrechtseingriffe in Bezug auf das Recht der informationellen Selbstbestimmung und die allgemeine Handlungsfreiheit gleichermaßen statt.[161]

Darüber hinaus kommen hier durch die automatische Detektion von Gesichtern und ihr Abgleich in Datenbanken sowohl eine erhöhte Eingriffsintensität als auch Eingriffe in weitere Grundrechte in Betracht.[162] In der Literatur wird dahingehend angebracht, dass Gesichtserkennung oder ein flächendeckender Einsatz entsprechender Software das Potenzial hat einen Verstoß gegen Art. 1 I GG darzustellen. Die Entwürdigung findet auf zwei Wegen statt. Zum einen dadurch, dass der Mensch grundsätzlich als Risiko behandelt wird und zum anderen, durch die technische Möglichkeit diverse Informationserhebungen zur Erstellung von Persönlichkeitsprofilen aufzeichnen zu können.[163]

Es besteht Einigkeit darüber, dass diese Kritik „eher symbolischen Charakter“[164] hat und „intelligente Videoüberwachung nicht *per se* entwürdigend“[165] ist. Aber gerade die biometrische Identifizierung durch Gesichtserkennungssoftware ist nicht harmlos oder unproblematisch und hat je nach Einsatz(Modalität) zumindest Eingriffspotenzial.[166]

Des Weiteren bestehen Bedenken gegen die Vereinbarkeit intelligenter Videoüberwachung mit dem Gleichheitsgrundsatz aus Art. 3 GG. Ein Algorithmus, der den Kontrollblick ersetzt, muss sich am Maßstab des Gleichheitsgrundsatzes messen lassen.[167] Fraglich ist die intelligente Videoüberwachung im Rahmen biometrischer Detektion auffälliger Verhaltensweisen, da sie zum Beispiel Behinderte nicht ausnimmt und angesichts polizeilicher Statistiken im Bereich der Gewalttaten voraussichtlich überwiegend Männer fokussieren würde.[168]

---

[161] Vgl. zum Eingriff in das Recht auf informationelle Selbstbestimmung und die allg. Handlungsfreiheit durch intelligente Videoüberwachung ausführlich *Held*, Intelligente Videoüberwachung, 78 – 109.
[162] Vgl. *Held*, Intelligente Videoüberwachung, 216.
[163] Vgl. *Ammicht Quinn*, Intelligente Videoüberwachung: eine Handreichung, https://publikationen.uni-tuebin-gen.de/xmlui/bitstream/handle/10900/67099/Band11_Vidoe%C3%BCberwachung_Handreichung.pdf?sequence=1, (06.10.2017), 36.
[164] *Ammicht Quinn*, Intelligente Videoüberwachung: eine Handreichung, https://publikationen.uni-tuebin-gen.de/xmlui/bitstream/handle/10900/67099/Band11_Vidoe%C3%BCberwachung_Handreichung.pdf?sequence=1, (06.10.2017), 36.
[165] *Held*, Intelligente Videoüberwachung, 76.
[166] Vgl. *Held*, Intelligente Videoüberwachung, 77, 217.
[167] Vgl. *Held*, Intelligente Videoüberwachung, 162.
[168] Vgl. dazu ausführlich *Held*, Intelligente Videoüberwachung, 166ff.

Ist die Gesichtserkennung in einer Videoüberwachungsanlage integriert, wird sie nicht nur rechtsstaatlich, sondern auch datenschutzrechtlich zur Herausforderung. Entscheidend für die Eingriffsintensität sind, wie bereits dargestellt, unter anderem die technischen Möglichkeiten und Anwendungen. Nach der Eingriffsintensität richtet sich auch die datenschutzrechtliche Relevanz.[169] Hinzu kommt, dass ein technischer Vorgang nur dann datenschutzrechtlich Bedeutsamkeit erlangt, wenn somit gewonnene Daten weiterverarbeitet werden. Wenn also eine Person nicht nur schlichtweg visuell erfasst wird, sondern zum Beispiel nachfolgend auch überwacht, beobachtet oder im Klarbild übertragen wird, während andere ohne Weiteres ausgesondert werden.[170] Diese Tatsache eröffnet, wie schon bei der einfachen Videoüberwachung, den Anwendungsbereich von § 6 b BDSG. Die Erfordernisse zum Schutz der Privatheit in Form von Zweckbindung und Verhältnismäßigkeit der Datenverarbeitung müssen demnach gewährleistet sein, nur dann liegt kein datenschutzrechtlicher Verstoß vor.[171]

Die Gesichtserkennung und der Lichtbildvergleich stützen sich auf unterschiedliche Ermächtigungsgrundlage, obwohl sie beide zu den kriminaltechnischen Untersuchungen zählen. Die computergestützte Gesichtserkennung legitimiert sich über den § 98 c StPO. Demnach dürfen zur Aufklärung einer Straftat personenbezogene Daten maschinell mit bereits gespeicherten Daten abgeglichen werden. Dazu zählt eben auch, dass Lichtbilder mit dem Datenbestand der erkennungsdienstlichen Behandlungen abgeglichen werden dürfen. Die Eingriffsintensität ist sehr gering, weil ausschließlich bereits vorhandenes Wissen genutzt wird. Es gibt daher keine Subsidiaritätsklausel, keinen Straftatenkatalog oder außerordentliche Anordnungskompetenz.[172] Der Lichtbildvergleich stützt sich auf die Generalklausel § 163 I S. 1 StPO, da es für die Erstellung eines morphologischen Gutachtens keine spezialgesetzliche Regelung gibt.[173]

---

[169] Vgl. *Bretthauer*, Intelligente Videoüberwachung, 94.
[170] Vgl. *Bretthauer*, Intelligente Videoüberwachung, 103f.; vgl. *BVerfG*, Urteil vom 11.03.2008 – Rs. 1 BvR 2074/05.
[171] Vgl. *Bretthauer*, Intelligente Videoüberwachung, 122; 128.
[172] Vgl. *Ahlbrecht* in: *Gercke et al.*, Heidelberger Kommentar zur Strafprozessordnung, 453f.
[173] Vgl. *Zöller* in: *Gercke et al.,* Heidelberger Kommentar zur Strafprozessordnung, 1146.

4 Die Öffentlichkeitsfahndung

Nach den Ermittlungsmethoden der Gesichtserkennung soll nun noch die Öffentlichkeitsfahndung dargestellt werden. Pauschal definiert ist die Öffentlichkeitsfahndung, die „Suche nach Personen oder Sachen unter Inanspruchnahme der Bevölkerung im Rahmen der Strafverfolgung und der Gefahrenabwehr.“[174]

Die Strafverfolgungsbehörden erhoffen sich durch Öffentlichkeitsfahndungen neue Ermittlungsansätze. Ein solcher Aufruf impliziert einen Appell an die Bürger, bedeutsame Beobachtungen sowie tatrelevantes Wissen mitzuteilen und bei der Aufklärung strafbarer Handlungen mitzuwirken. Die Staatsanwaltschaft kann sogar monetäre Anreize geben, indem sie eine Belohnung für sachdienliche Hinweise auslobt.[175] Die Öffentlichkeitsfahndung wird bewusst sparsam eingesetzt, um das Ermittlungsinstrument nicht zu verschleißen. Würde die Bevölkerung allzu oft mit Fahndungsaufrufen konfrontiert, könnte ein Gewöhnungs- und Abnutzungseffekt eintreten.[176]

Bei strafprozessualen Öffentlichkeitsfahndungen lassen sich drei Zielrichtungen unterscheiden. Es gibt die Öffentlichkeitsfahndung zur Festnahme, wobei die Personalien des Gesuchten bereits feststehen, es gibt die Fahndung zur Aufenthaltsermittlung und es gibt die Ermittlungsöffentlichkeitsfahndung, auch Aufklärungsfahndung genannt. Bei letzterer soll durch die Fahndung, die Identität eines unbekannten Täters oder Zeugen festgestellt werden.[177] Dazu wird ein Bild der gesuchten Person publiziert.[178] Die Aufklärungsfahndung wird deshalb für den Bereich Öffentlichkeitsfahndung im empirischen Part zur Auswertung ihrer Effizienz herangezogen.

4.1 Kriminalistische Relevanz

Etymologisch geht das Wort fahnden auf das mittelniederdeutsche Wort *vanden* für besuchen und in weiterer Wortverwandtschaft auf das Verb finden zurück. Zudem findet sich in dem Wort fahnden der Einfluss des Wortes fangen wieder, welches von dem Wort *fahen* abstammt. Die Fahndung im Sinne der

---

174 *Wirth*, Kriminalistik-Lexikon, 409.
175 Vgl. *Walder/Hansjakob*, Kriminalistisches Denken, 274.
176 Vgl. *Averdiek-Gröner/Frings*, Standardmaßnahmen im Ermittlungsverfahren, 130.
177 Vgl. *Wirth*, Kriminalistik-Lexikon, 409; *Averdiek-Gröner/Frings*, Standardmaßnahmen im Ermittlungsverfahren, 131.
178 Vgl. *Wirth*, Kriminalistik-Lexikon, 409.

polizeilichen Suchaktion hat sich ohne direkten Zusammenhang zu diesen Wortbedeutungen, obwohl sie sehr zutreffen, Anfang des 19. Jahrhunderts neu herausgebildet.[179]

Im Gesamtkonstrukt Fahndung ist die Öffentlichkeitsfahndung eine von vielen möglichen Varianten.[180] Für welche Fahndungsart sich ein Beamter im Verfahren oder Ersten Angriff entscheidet, hängt von verschiedenen Faktoren ab. Ausschlaggebend ist beispielsweise die Schwere der Tat, das Bestehen bedeutender Informationsdefizite oder das Vorliegen der entsprechenden rechtlichen Voraussetzungen.[181]

Was die Öffentlichkeitsfahndung ist und wann sie in Betracht kommt, das definiert die Kriminalistik für sich detaillierter als bisher dargestellt und beschreibt sie als „eine gezielte, repressiven oder präventiven Zwecken dienende Suche nach Personen oder Sachen unter Inanspruchnahme einer bestimmten Zielgruppe oder eines unbestimmten Teils der Bevölkerung.“[182] Sie differenziert mithin in die zielgruppenorientierte und die allgemeine Öffentlichkeitsfahndung. Der kriminaltaktische Vorteil eine Fahndung nur an bestimmte Personen zu richten, liegt darin, dass sie dem Täter vermutlich verborgen bleibt und er sein Verhalten nicht ändern, beziehungsweise an Fahndungsmaßnahmen anpassen kann. Ein allgemeiner öffentlicher Aufruf kann hingegen sowohl positive als auch negative Folgen für das Ermittlungsverfahren haben. So ist ein Fahndungsaufruf an die Gesamtbevölkerung geeignet, den Täter zu verunsichern. Er kann zudem weitere Opfer und Zeugen zur Aussage motivieren. Andererseits sind die möglichen negativen Auswirkungen nicht unerheblich. Da wäre zum einen die Warnung des Täters, aber auch seine Stigmatisierung. Vor allem aber spielt die Sekundärviktimisierung für Opfer und die Gefahr von Trittbrettfahrern sowie die Behinderung der weiteren polizeilichen Ermittlungen eine große Rolle.[183] Die zielgruppenorientierte Öffentlichkeitsfahndung ist auch von minderer Eingriffsintensität, weshalb ihr vor der allgemeinen Öffentlichkeitsfahndung der Vorrang zu gewähren ist.[184]

---

[179] Vgl. https://www.dwds.de/wb/fahnden, (21.10.2017); vgl. auch *Störzer*, Zur Geschichte der Fahndung, IX.
[180] Vgl. *Clages/Ackermann*, Der rote Faden, 270.
[181] Vgl. *Clages/Ackermann*, Der rote Faden, 273.
[182] *Wirth*, Kriminalistik-Lexikon, 410.
[183] Vgl. *Wirth*, Kriminalistik-Lexikon, 410.
[184] Vgl. *Clages/Ackermann*, Der rote Faden, 282.

Es gibt weitere grundsätzliche Probleme, die mit einer Inanspruchnahme der Bevölkerung zur Strafverfolgung einhergehen. Es müssen im Rahmen der Öffentlichkeitsfahndung Ermittlungsinformationen preisgegeben werden, anhand derer sich auch der Täter ein Bild über den Kenntnisstand der Polizei machen kann. Das ist ein taktischer Nachteil für die Ermittlungsbehörden. Es kann sich nach erfolgreicher Fahndung und einem geständigen Tatverdächtigen zusätzlich im späteren Verlauf des Verfahrens das Problem ergeben, dass im Fall eines Widerrufs des Geständnisses behauptet werden kann, das Wissen über die Tat stamme aus den medialen Fahndungsaufrufen der Polizei. Im Nachgang wird das schwer zu widerlegen sein.[185]

Die Maßnahme der Öffentlichkeitsfahndung ist nur dann wirklich sinnvoll, wenn angenommen werden kann, dass es noch jemanden gibt, der Informationen zu einem Tatgeschehen geben kann. Diesbezüglich gibt es nur drei Möglichkeiten. Zum einen könnte es noch Zeugen geben, die ihre Wahrnehmungen bisher für irrelevant gehalten haben. Zum anderen könnte es ein, dass der Fahndungsaufruf potenzielle Hinweisgeber motiviert, doch noch zur Polizei zu gehen. Bei diesen Zeugen ist aber Vorsicht geboten, insbesondere in Verbindung mit einer Belohnung, denn normalerweise würde sich jemand, der bei der Aufklärung einer Straftat helfen will auch ohne extrinsischen Anstoß melden. Gegenüber einer auf diesem Weg getätigten Aussage, sollte ein gesundes Misstrauen herrschen. Am sinnvollsten ist eine Öffentlichkeitsfahndung bei der dritten Konstellation. Hier liegt Bildmaterial zum Tatgeschehen vor, aufgrund dessen man sich eine Identifizierung der abgebildeten Personen durch die Bevölkerung erhofft. Bei einer guten Bildqualität, wird in der Literatur sogar von einer hohen Wahrscheinlichkeit der Identifizierung gesprochen.[186]

Die allgemeinen Fahndungsaufrufe werden im Internet, der Druckpresse, dem Fernsehen und anderen generell zugänglichen Medien und Quellen publiziert. Dementsprechend unterscheidet man im Verbreitungsgrad noch zwischen lokal, regional und überregional.[187]

---

[185] Vgl. *Walder/Hansjakob*, Kriminalistisches Denken, 274.
[186] Vgl. *Walder/Hansjakob*, Kriminalistisches Denken, 275.
[187] Vgl. *Clages/Ackermann*, Der rote Faden, 282f.

Historisch gesehen, blickt die Öffentlichkeitsfahndung im Zusammenhang mit (Straf-)Verfolgung auf eine lange Vergangenheit zurück. Weit vor der Entstehung der Begrifflichkeit, gab es bereits Verfahren, die der Maßnahme im heutigen Sinne glichen. So finden sich bereits im alten Ägypten etwa 145 v. Christus Hinweise auf Ausschreibungen entlaufener Sklaven mit Personenbeschreibungen und Skizzen sowie dem Versprechen einer Belohnung für die Nennung des Aufenthaltsortes.[188] Anfang des 17. Jahrhunderts wiederum schrieb William Shakespeare in „König Lear“ folgende Passage:[189]

„Flieh' er noch so weit,
In diesem Land entgeht er nicht der Haft,
Und, trifft man ihn, der Strafe. (…)
Daß, wer ihn findet, unsern Dank verdient,
Bringt er den feigen Meuchler zum Gericht:
Wer ihn verbirgt, den Tod. (…)
Die Häfen sperr' ich all', er soll nicht fliehn.
Mein Fürst muß mir's gewähren; auch sein Bildnis
Versend' ich nah und fern; das ganze Reich
Soll Kenntnis von ihm haben (…).“[190]

Das deutet daraufhin, dass die heutigen Fahndungsmaßnahmen, in ihrer konkreten Ausgestaltung, weit zurückreichend verwurzelt sind.
Fahndungsausschreibungen wurden früher auch Steckbriefe genannt.[191] In diesem Zusammenhang spielt die Daguerreotypie, ebenso wie bei der Gesichtserkennung, eine Rolle.[192] Die erste richtige fotografische Methode brachte auch die Fahndung nach Straftätern voran und ermöglichte es 1843 den Belgiern als Vorreiter, Steckbriefe mit Bildnissen in Form von Ablichtungen zu versehen.[193]

---

[188] Vgl. *Heindl*, System und Praxis der Daktyloskopie und der sonstigen technischen Methoden der Kriminalpolizei, 538f.
[189] Vgl. *Kube*, Beweisverfahren und Kriminalistik in Deutschland, 133.
[190] *Shakespeare*, König Lear, 33f.; vgl. *Kube*, Beweisverfahren und Kriminalistik in Deutschland, 133; vgl. *Störzer*, Zur Geschichte der Fahndung, XIf.
[191] Vgl. *Beulke*, Strafprozessrecht, 184.
[192] Vgl. *Kube*, Beweisverfahren und Kriminalistik in Deutschland, 133.
[193] Vgl. *Mergen*, Die Wissenschaft vom Verbrechen, 33.

4.2 Intranet-Fahndung als Exkurs

Für Polizeibeamte gibt es ein geschlossenes Datennetzwerk, das Intranet.[194] Ein Intranet ist analog zum Internet omnipotent und kann flexibel auf die Anwendungsbereiche eines Unternehmens oder einer Behörde zugeschnitten werden.[195] So ein Datennetzwerk unterstützt die innerbetriebliche Kommunikation.[196] Es ermöglicht folglich eine Zusammenarbeit über Zuständigkeitsgrenzen hinaus. Die Kommunikation der Mitarbeiter gehört zur Organisationskommunikation im gesamten. Ihre Ausgestaltung kann wesentlich zu dem Erfolg einer Organisation und zum Erreichen ihrer Ziele beitragen.[197] So ist es auch bei den Strafverfolgungsorganen. Polizisten sind dank des Intranets besser und schneller miteinander verknüpft.[198] Das polizeiinterne Datennetz dient den Beamten zum Beispiel zur Weitergabe landesinterner, spezifischer Dienstvorschriften oder zum Informationsaustausch. Mithin kann es zu Fahndungszwecken hilfreich sein.[199] Es ist jedem Sachbearbeiter möglich, Bildmaterial aus einem Ermittlungsverfahren über das interne Netzwerk zugänglich zu machen. Das Fahndungsersuchen eines Ermittlers wird dort nur für Kollegen einsehbar, wodurch es der Maßnahme an Offenheit und mithin an Öffentlichkeit fehlt.[200]

Die Intranet-Fahndung muss der „medienunterstützten Fahndung im weiteren Sinne“[201] zugeordnet werden. Durch sie besteht die Chance, dass Straftaten durch eine polizeiinterne Veröffentlichung von Bildmaterial, welches am Tatort oder im Tatortnahbereich gefertigt wurde, durch den Kollegenkreis aufgeklärt werden können, bevor die Bilder die breite Öffentlichkeit erreichen. Sie ist mithin keine Öffentlichkeitsfahndung, obgleich sie ihr vom Prinzip her ähnelt.[202] Will man den Beitrag der Videoüberwachung zur Kriminalistik beurteilen, dann darf dieses Fahndungshilfsmittel nicht gänzlich außer Acht gelassen werden.

---

194 Vgl. *Soinè*, Ermittlungsverfahren und Polizeipraxis, 78.
195 Vgl. *Meier et al.*, Herausforderung Intranet, 3.
196 Vgl. *Rommert*, Hoffnungsträger Intranet, 83; 86.
197 Vgl. *Hoffmann*, Das Intranet, 17; 28.
198 Vgl. *Schneider*, Polizeiliche Fahndung – neue Wege zum Erfolg, 25.
199 Vgl. *Soinè*, Ermittlungsverfahren und Polizeipraxis, 78.
200 Vgl. *LG Berlin*, Beschluss vom 17. Dezember 2008, Az.: 501 Qs 208/08; vgl. *Wirth*, Kriminalistik-Lexikon, 438; vgl. *Soinè*, Ermittlungsverfahren und Polizeipraxis, 78.
201 *Benfer/Bialon*, Rechtseingriffe von Polizei und Staatsanwaltschaft, 281.
202 Vgl. *Schneider*, Polizeiliche Fahndung – neue Wege zum Erfolg, 25.

4.3 Rechtliche Einordnung

Die Bestimmungen zur strafprozessualen Öffentlichkeitsfahndung sind in den §§ 131 ff. StPO geregelt. Wird eine Fahndung mit dem Ziel der Festnahme eines Beschuldigten abgesetzt, dann richtet sich der Aufruf nach § 131 StPO. Soll durch die Fahndung bezweckt werden, den Aufenthaltsort einer bekannten Person zu bestimmen, dann ist § 131 a StPO einschlägig. Die Aufklärungsfahndung zur Feststellung der Identität eines unbekannten flüchtigen Tatverdächtigen oder unbekannten Zeugen richtet sich nach § 131 b StPO.[203]
Da es im Weiteren wesentlich um diese Ermittlungsöffentlichkeitsfahndung gehen wird, sollen ihre Voraussetzungen kurz skizziert werden. § 131 b I StPO erlaubt die Veröffentlichung von Bildmaterial eines unbekannten Tatverdächtigen, wenn die Identität anders nur schwer festgestellt werden kann oder sie voraussichtlich unbekannt bleibt. Man spricht insofern von Subsidiarität der Maßnahme. Es ist zudem erforderlich, dass dem Strafverfahren und der Fahndungsmaßnahme eine Straftat von erheblicher Bedeutung zugrunde liegt.[204] Was eine Straftat von erheblicher Bedeutung darstellt, ist nicht detailliert definiert. Es gibt diesbezüglich keinen Deliktskatalog. Vielmehr ist es erforderlich sich an dazu ergangener Rechtsprechung zu orientieren. Bagatelldelikte und fahrlässig begangene Straftaten sind ausgeschlossen, so dass es sich mindestens um eine Verfehlung des mittleren Kriminalitätsbereiches handeln muss.[205] § 131 b II S. 1 StPO ermöglicht in diesem Zusammenhang auch nach unbekannten Zeugen zu fahnden. Hierbei gelten die gleichen Anforderungen an die Straftat. Die Anforderungen an die Subsidiarität hingegen sind verschärft. Der öffentliche Aufruf nach der Identität eines Zeugen mit seinem Abbild darf nur dann stattfinden, wenn man anders nahezu unmöglich an seine Personalien kommt. Gemäß § 131 II S. 2 StPO ist es unabdingbar, explizit darauf hinzuweisen, dass es sich bei der gesuchten Person um einen Zeugen handelt. Die Anordnung und Bestätigung einer Aufklärungsfahndung obliegt nach § 131 c I StPO dem Richter. Nur bei Gefahr im Verzuge darf die Anordnung durch einen Staatsanwalt oder seine Ermittlungspersonen erfolgen. Die

[203] Vgl. *Burhoff*, Handbuch für das strafrechtliche Ermittlungsverfahren, 932.
[204] Vgl. *Burhoff*, Handbuch für das strafrechtliche Ermittlungsverfahren, 935f.
[205] Vgl. *Burhoff*, Handbuch für das strafrechtliche Ermittlungsverfahren, 933.

Anordnungskompetenz liegt beim Richter, weil die Ermittlungsöffentlichkeitsfahndung einen schweren Eingriff in die Persönlichkeitsrechte des Täters darstellt. Durch die Veröffentlichung von Abbildungen einer Person im Zusammenhang mit einer Straftat, kann sie erheblich in ihrem Recht auf freie Entfaltung der Persönlichkeit verletzt werden. Die Person kann nicht mehr selbst darüber bestimmen, ob gewisse Dinge aus ihrem Leben der Öffentlichkeit zugänglich sind. Denkbar ist auch die Einschränkung der allgemeinen Handlungsfreiheit der von der Fahndung betroffenen Person. Persönlichkeitsrechte und Freiheitsrechte werden vom Grundgesetz jedoch nur soweit gewährt, wie sie nicht gegen die verfassungsmäßige Ordnung gehen.[206] „Folglich hat jedermann im Rahmen seiner Gemeinschaftsbezogenheit staatliche Maßnahmen zu dulden, die im überwiegenden Interesse der Allgemeinheit unter strikter Wahrung des Verhältnismäßigkeitsgrundsatzes erfolgen (…).“[207]

Durch die öffentliche Abbildung von Tatverdächtigen durch Strafverfolgungsbehörden ist auch ein Verstoß gegen die §§ 22, 23 KUG denkbar. Ein Bildnis darf danach nur veröffentlicht werden, wenn die abgebildete Person ihre Einwilligung erteilt hat. Einer Einwilligung bedarf es dann nicht, wenn eine der Ausnahmen gem. § 23 KUG vorliegt. Das ist der Fall, wenn es sich zum einen um Bildnisse der Zeitgeschichte, der Kunst oder von Versammlungen etc. handelt oder zum anderen eine Person auf dem Bild gar nicht Mittelpunkt, sondern nur Beiwerk ist. Ein Verstoß gegen Urheberrechte liegt im Zusammenhang mit einer Öffentlichkeitsfahndung insoweit nicht vor, da § 24 KUG Behörden berechtigt, zum Zweck der Rechtspflege und zum Schutz der öffentlichen Sicherheit, Bilder ohne Einwilligung zu publizieren.[208] Es wird zudem argumentiert, dass es sich bei der Veröffentlichung von Bildern unbekannter Tatverdächtiger im Zusammenhang mit der Verfolgung schwerwiegender Straftaten um Bilder aus dem Bereich der Zeitgeschichte gem. § 23 I Ziff. 1 KUG handeln kann, da es ein Anliegen der Öffentlichkeit ist, Täter solcher Delikte zur Rechenschaft zu ziehen. Denn der Begriff Zeitgeschichte bezieht sich nicht auf historische Relevanzen, sondern darauf, was gegenwärtig gesellschaftlich interessiert.[209]

---

[206] Vgl. *Benfer/Bialon*, Rechtseingriffe von Polizei und Staatsanwaltschaft, 279.
[207] *Benfer/Bialon*, Rechtseingriffe von Polizei und Staatsanwaltschaft, 279.
[208] Vgl. *Von Becker*, Straftäter und Tatverdächtige in den Massenmedien, 143.
[209] Vgl. *Benfer/Bialon*, Rechtseingriffe von Polizei und Staatsanwaltschaft, 290.

Seit es auf dem Gebiet der Fahndung die Möglichkeit gibt ein Bild mit den entsprechenden Informationen im World Wide Web zu veröffentlichen, besteht die Gefahr einer dauerhaften Stigmatisierung abgelichteter Personen mehr als je zuvor. Dadurch, dass dieses Medium schwer begrenzbar ist und Nachrichten schnell viral gehen, kann hier ein Eingriff in die Persönlichkeitsrechte etwas schwerer wiegen als bei einer Veröffentlichung über die altbewährten Medien. Im Rahmen der Verhältnismäßigkeit muss dieser Tatsache gebührend Rechnung getragen werden.[210] Gesetzlich wurde dieser Umstand in § 131c II StPO verankert, der die andauernde Veröffentlichung in elektronischen Medien regelt und eine zeitnahe richterliche Bestätigung einer staatsanwaltlichen Anordnung verlangt.[211] Das große Risiko bei Internetveröffentlichungen vor allem im Web 2.0 ist, dass die Daten global abruf- und verbreitbar sind. Sobald Daten darüber veröffentlicht werden, sind sie nicht mehr steuerbar.[212] Sie können also nicht mit Sicherheit wieder gelöscht werden, obwohl die Beendigung der Fahndung vorgeschrieben ist.[213] Die Daten werden zudem an eine außerbehördliche, amerikanische Übermittlungsstelle weitergegeben, die nicht dieselben Anforderungen an das Datenschutzniveau hat, wie die EU.[214] Der Zweck der Strafverfolgung heiligt in diesem Fall nicht das Mittel, denn gem. § 4 c I BDSG ist eine solche Weitergabe der Daten nur legitim, wenn der „Anwendungsbereich des Rechts der Europäischen Gemeinschaft“[215] eröffnet ist. Strafverfolgungsorgane nehmen bei Facebook-Fahndungen bewusst den Kontrollverlust zur Aufklärung von Straftaten in Kauf. Letztlich lassen sich datenschutzrechtliche Verstöße wie der oben genannte gegen das Übermittlungsverbot nur mit einem überwiegenden Interesse der Allgemeinheit an einer schnellen Tataufklärung sowie dem generalpräventiven Schutz der Bevölkerung vor weiteren Straftaten rechtfertigen.[216]

Bei der Intranet-Fahndung hingegen droht, durch ihre Begrenztheit, kein Kontrollverlust der Daten. Hier ist die Eingriffsintensität grundsätzlich sogar geringer einzuschätzen als bei der Öffentlichkeitsfahndung, da das Bildmaterial und die Einzelheiten zu einem Tatgeschehen nur einem begrenzten Personenkreis

---

[210] Vgl. *Ströbel*, Persönlichkeitsschutz von Straftätern im Internet, 61.
[211] Vgl. *Gercke et al.*, Heidelberger Kommentar zur Strafprozessordnung, 857.
[212] Vgl. *Bajmel*, Datenschutz in sozialen Netzwerken, 17.
[213] Vgl. *RiStBV*, Anlage B, Ziff. 2.1 und 3.2.
[214] Vgl. *Bajmel*, Datenschutz in sozialen Netzwerken, 169.
[215] *Bajmel*, Datenschutz in sozialen Netzwerken, 169.
[216] Vgl. *Bajmel*, Datenschutz in sozialen Netzwerken, 174f.

zur Kenntnis gelangen. Das AG Bonn konstatiert in einem Beschluss vom 21.04.2016, dass Veröffentlichungen im polizeilichen Intranet nicht genehmigungsbedürftig sind.[217] Das heißt, streng genommen, dass sich diese Veröffentlichungen nicht nach §§ 131 ff. StPO richten, keine Ausschreibungen darstellen und somit wesentlich niedrigschwelliger anzusetzen sind. Die Feststellung des Amtsgerichtes Bonn ist entscheidend, da sie bedeutet, dass bei polizeiinternen Fahndungen nach unbekannten Tatverdächtigen keine staatsanwaltliche Anordnung erforderlich ist. Folgt man der Meinung von *Benfer* und *Bialon*, dann handelt es sich bei der Intranet-Fahndung um ein Fahndungshilfsmittel, welches sich über die Generalklausel § 163 StPO legitimiert.[218] Daneben konstatieren *Clages* und *Ackermann* einhellig, dass die Fahndung im Allgemeinen, und somit auch die interne, als Generalauftrag gem. § 163 StPO zur Strafverfolgung zu verstehen ist.[219]

Die präventive Öffentlichkeitsfahndung, zum Beispiel bei Vermisstensachen, ergibt sich aus den landes- und bundesspezifischen Regelungen der jeweiligen Polizeigesetze. Wenige Länder haben die Öffentlichkeitsfahndung dabei explizit benannt. Zu diesen Ausnahmen gehören folgende Ermächtigungsgrundlagen: § 36 II Nr. 1 BremPolG, § 41 II Nr. 1 SOG M-V, § 44 II Nr. 1 Nds. SOG und § 34 VII POG RP. Die Mehrheit der Länder stützt diese Maßnahme jedoch auf eine allgemeine Vorschrift zur Datenübermittlung. Dazu gehören § 32 IV BPolG, § 44 I Nr. 3 PolG BW, Art. 41 I Nr. 3 BayPolG, § 45 I Nr. 3 ASOG Bln, § 44 I Nr. 2 BbgPolG, § 21 I Nr. 2 HmbPolDVG, § 23 I Nr. 3 HSOG, § 29 I Nr. 2 PolG NRW, § 34 I S. 2 SPolG, § 45 I SächsPolG, § 28 I Nr. 3 SOG LSA i.V.m. § 26 III SOG LSA, § 193 I S. 2 LVwG SH, § 41 III S. 2 TH PAG.[220] Weiterhin gelten für die polizeiliche Fahndung die Bestimmungen des Abschnittes I, Punkt 5, Nummer 39 – 43 der RiStBV sowie Anlage B zur RiStBV für die Öffentlichkeitsfahndung[221] und die Polizeidienstvorschriften 384.1 (Fahndung) und 389 (Vermisste). Polizeidienstvorschriften sind nur für den Dienstgebrauch und werden daher nicht näher ausgeführt.[222]

---

[217] Vgl. *AG Bonn*, Öffentlichkeitsfahndung – erhebliche Straftat, 248.
[218] Vgl. *Benfer/Bialon*, Rechtseingriffe von Polizei und Staatsanwaltschaft, 287; ähnlich zum allgemeinen Fahndungsauftrag der Polizei *Clages/Ackermann*, Der rote Faden, 269.
[219] Vgl. *Clages/Ackermann*, Der rote Faden, 269.
[220] Vgl. *Wirth*, Kriminalistik-Lexikon, 410.
[221] Vgl. *Kube et al.*, Kriminalistik, Bd. 2, 225.
[222] Vgl. *Clages/Ackermann*, Der rote Faden, 266.

5 Nationale und internationale Forschung

Die drei Komplexe Videoüberwachung, Gesichtserkennung und Öffentlichkeitsfahndung sind zum Teil breit erforscht. Wie eingangs erwähnt, ist das große wissenschaftliche Interesse an der Videoüberwachung interdisziplinär. Sie wird bereits Jahrzehnte aus verschiedenen Perspektiven untersucht. Seit geraumer Zeit wird sie, durch den technologischen Fortschritt bedingt, auch in Bezug auf den Mehrwert und die Funktionalität integrierter Gesichtserkennungssoftware studiert.[223] Es überrascht daher nicht, dass in den letzten Jahren entsprechend auch die Gesichtserkennung in ihrer technischen Ausgestaltung einem ständigen Verbesserungsprozess unterliegt.[224] Es gibt eine Webseite auf der Wissenschaftler ihre Forschungsvorhaben rund um Überwachung, Technologie und Kontrolle kartografisch angeben können. Das Portal dient der Vernetzung und besseren Kommunikation unter Wissenschaftlern.[225] Das Feld der Öffentlichkeitsfahndung und der polizeiinternen Fahndungshilfsmittel ist hingegen in der Vergangenheit offiziell gar nicht Gegenstand empirischer Untersuchungen gewesen. Der folgende Abschnitt soll daher einen kleinen Überblick über interessante und bedeutsame Forschungen zu den Thematiken geben, ohne dabei Anspruch auf Vollständigkeit zu erheben.

Die Videoüberwachung ist vor allem soziokulturell erforscht. Nennenswert ist die quantitative Umfrage zu Videoüberwachung, Sicherheitsgefühl und Wahrnehmung von *Zurawski* in Hamburg. Sie wurde von 2003 bis 2007 durch die Deutsche Forschungsgemeinschaft gefördert.[226] Im Ergebnis stellen *Zurawski* und *Czerwinski* nach Befragungen von Passanten der Reeperbahn fest: „Videoüberwachung ist also nicht gleich Videoüberwachung. Politik (…) sollte sich differenziert, ergebnisoffen und am Einzelfall orientiert mit diesem Thema auseinandersetzen.“[227] Von 2010 bis 2013 lief das Forschungsprojekt Sicherheit im öffentlichen Raum (SIRA), welches versuchte, eine Bewertungsmethodik zu schaffen, wodurch zukünftige Sicherheitsmaßnahmen im Hinblick auf ihre Akzeptanz in der Bevölkerung optimiert werden können. Es handelte sich

---

[223] Vgl. *Humer/Lederer*, Von der konventionellen zur intelligenten Videoüberwachung, 36.

[224] Vgl. zum geschichtlichen Überblick einiger Forschungsvorhaben *Bundesamt für Sicherheit in der Informationstechnik,* https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Biometrie/Gesichtserkennung_pdf.pdf?__blob=publicationFile, (29.10.2017).

[225] Vgl. *Zurawski*, http://www.surveillance-studies.org/forschernetzwerk/forschungsstandorte-surveillance-studies/, (29.10.2017).

[226] Vgl. *Deutsche Forschungsgemeinschaft*, http://gepris.dfg.de/gepris/projekt/5405691, (29.10.2017).

[227] *Zurawski/Czerwinski*, Sie sind doch auch für Videoüberwachung, oder…? 220.

dabei um ein Verbundprojekt mit mehreren Teilvorhaben. Eines der Teilvorhaben beschäftigte sich mit der datenschutzgerechten Gestaltung von Sicherheitstechnik. Das Gesamtprojekt wurde durch das Bundesministerium für Bildung und Forschung gefördert.[228] Einen sozialwissenschaftlichen Forschungsbeitrag zur Akzeptanz von Videoüberwachung lieferte auch *Kudlacek* 2015. Dort findet sich eine detaillierte Darstellung weiterer empirischer Untersuchungen zur Überwachung öffentlicher Räume mit dem Anknüpfungspunkt der gesellschaftlichen Akzeptanz.[229] Sein Fazit ist, dass Videoüberwachung mehrheitlich positiv bewertet wird und dass die Bevölkerung an intelligente und automatisierte Formen einer solchen, hohe Erwartungen knüpft.[230] Auf europäischer Ebene wurde Anfang der 2000er Jahre mit dem Großprojekt Urbaneye in mehreren Ländern der Nutzen sowie soziale und politische Konsequenzen von Videoüberwachung untersucht. Teilbereiche der Forschung waren beispielsweise Akzeptanz, Einstellung und Vertrauen der Bevölkerung gegenüber der Technik sowie ihre Risiken, auch in Bezug auf Bürgerrechte.[231] Seit 2009 gibt es mit INDECT ein weiteres Projekt der EU. Dieses dreht sich zu einem großen Teil um die Entwicklung von Algorithmen und Software im Kampf gegen Verbrechen und um die Entwicklung datenschutzgerechter Sicherheitssysteme.[232] Jüngere Studien im Zusammenhang mit Videoüberwachung beschäftigen sich inzwischen schwerpunktmäßig generell weniger soziokulturell als mehr technisch. So folgten im vergangenen Jahrzehnt vermehrt Studien zur Gesichtserkennung und Biometrie in Verbindung mit Videoüberwachung. Das Bundeskriminalamt initiierte 2005-2007 ein Forschungsprojekt mit dem Titel „Gesichtserkennung als Fahndungshilfsmittel. Foto-Fahndung." Dabei wurden Gesichtserkennungssysteme im Echtbetrieb am Mainzer Hauptbahnhof auf ihre Zuverlässigkeit getestet. Zudem wurden Algorithmen auf ihre Eignung erprobt, Live-Bilder mit einer Referenzdatenbank in Echtzeit abzugleichen.[233] Die Systeme erreichten bei Tageslicht eine Trefferquote von

---

[228] Vgl. *Bundesministerium für Bildung und Forschung*, https://www.sifo.de/de/sira-sicherheit-im-oeffentlichen-raum-1868.html, (29.10.2017).
[229] Vgl. *Kudlacek*, Akzeptanz von Videoüberwachung, 44ff.
[230] Vgl. *Kudlacek*, Akzeptanz von Videoüberwachung, 149.
[231] Vgl. *Hempel/Töpfer*, http://www.urbaneye.net/results/ue_wp15.pdf, (29.10.2017).
[232] Vgl. o. V., homepage, http://www.indect-project.eu/, (29.10.2017).
[233] Vgl. *Bundeskriminalamt*, http://www.cytrap.eu/files/EU-IST/2007/pdf/2007-07-FaceRecognitionField-Test-BKA-Germany.pdf, 8, (29.10.2017).

etwa 70 Prozent. Bei schlechten Lichtverhältnissen nahm die Erkennungsleistung sogar noch stark ab.[234] Insgesamt stellten sich die Systeme folglich noch zu fehleranfällig für den Echtbetrieb dar. *Apelt* leitete von 2010 bis 2013 ein Verbundprojekt namens MuVit. Bei diesem Projekt wurden Mustererkennung und Video Tracking hinsichtlich ihrer sozialpsychologischen, soziologischen, ethischen und rechtlichen Vereinbarkeit in verschiedenen Teilvorhaben analysiert.[235] Bei diesem Forschungsvorhaben wurden außerdem diverse Anwendergruppen diskutiert, worunter auch die Polizei fiel.[236] Von 2012 bis 2014 gab es das vom Bundesministerium für Bildung und Forschung geförderte Programm MisPel: Multi-Biometriebasierte Forensische Personensuche in Lichtbild- und Videomassendaten. Das Projekt sollte unter anderem ermittlungsunterstützende Software für Videoüberwachungsanlagen nach Straftaten erarbeiten. Bei MisPel handelt es sich ebenfalls um ein Verbundprojekt mit mehreren interdisziplinären Teilvorhaben aus Sozial- und Rechtswissenschaft sowie Kriminalistik.[237] „Die polizeilichen Endanwender wurden aktiv in den Entwicklungsprozess eingebunden, denn die Skizzierung und iterative Weiterentwicklung der (…) Technik ist essentiell für einen erfolgreichen Gestaltungsprozess.“[238] Aktuell läuft, ähnlich dem Test von 2007 am Mainzer Hauptbahnhof, das Projekt „Sicherheitsbahnhof Berlin Südkreuz“ zur Erprobung aktueller, verbesserter Gesichtserkennungstechnik.[239]

Auch in Amerika werden Studien zur Gesichtserkennung durchgeführt und zum Teil staatlich gefördert. Dort begann das Interesse an dieser technischen Modifikation von Überwachungsanlagen bereits Mitte der 1990er Jahre. Im Departement of Defense wurden in dem Projekt FERET (Face Recognition Technology program) die ersten Testungen von Gesichtserkennungssystemen durchgeführt. Darauf baute eine Vielzahl weiterer Tests und Untersuchungen in den Folgejahren auf. Das National Institute for Standardization

---

[234] Vgl. *Bundeskriminalamt*, http://www.cytrap.eu/files/EU-IST/2007/pdf/2007-07-FaceRecognitionField-Test-BKA-Germany.pdf, 24, (29.10.2017).

[235] Vgl. *Bundesministerium für Bildung und Forschung*, https://www.sifo.de/de/muvit-mustererkennung-und-video-tracking-sozialpsychologische-soziologische-ethische-und-1950.html, (30.10.2017); vgl. *Apelt/Möllers*, Wie intelligente Videoüberwachung erforschen? 587.

[236] Vgl. *Hälterlein/Möllers*, Deutungskonflikte um automatisierte Videoüberwachung, 170.

[237] Vgl. *Bundesministerium für Bildung und Forschung*, https://www.sifo.de/de/mispel-multi-biometrieb-asierte-forensische-personensuche-in-lichtbild-und-videomassendaten-2105.html, (30.10.2017).

[238] *Humer/Lederer*, Von der konventionellen zur intelligenten Videoüberwachung, 37.

[239] Vgl. *Bundesministerium des Innern*, https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2017/08/gesichtserkennungstechnik-bahnhof-suedkreuz.html, (30.10.2017).

(NIST) erweiterte diese Untersuchungsreihen ebenso durch die Facial Recognition Grand Challenge (FRGC).[240] Auf der Webseite von NIST sind weitere aktuellere Forschungen zu den Thematiken Gesichtserkennung und Biometrie abrufbar.[241]

Die reine Technologie der Gesichtserkennung an sich wird auch außerhalb ihrer Integrität in Videoüberwachungsanlagen stets versucht zu optimieren. Die EU forschte 2006-2009 bereits an dreidimensionalen Gesichtserkennungsalgorithmen im Zusammenhang mit biometrischen Sicherheits- und Authentifizierungsmerkmalen in Ausweisdokumenten. Die daraus resultierenden Ergebnisse sind auch auf andere Anwendungsbereiche übertragbar.[242] Anfang der 2000er Jahre gab es desgleichen in Deutschland schon Untersuchungen durch das Bundesamt für Sicherheit in der Informationstechnik zum Vergleich von Gesichtserkennungssoftware (BioFace I und II)[243] und die Leistungsfähigkeit der Gesichtserkennung in Passdokumenten (BioP I und II)[244]. Die Fehleranfälligkeit von Gesichtserkennungssoftware in der praktischen Anwendung und ihre Grenzen sind der Forschung bewusst. Deshalb gab es Versuche, einige der Überlistungsmöglichkeiten technisch auszuräumen. Zum einen gab es bis 2015 ein Teilforschungsprojekt beim Bundeskriminalamt, welches eine 3D- Gesichtserkennung testete, um zukünftig auch Aufnahmen aus Überwachungskameras auswerten und mit Referenzdatenbanken abgleichen zu können, die die Täter nicht ausschließlich frontal zeigen.[245] Das ganze Verbundprojekt „GES-3D: Multi-Biometrische Gesichtserkennung“ wurde vom Bundesministerium für Bildung und Forschung gefördert.[246] Im Zusammenhang mit der Dreidimensionalität sei an dieser Stelle erwähnt, dass es ebenso

---

[240] Vgl. *Bundesamt für Sicherheit in der Informationstechnik*, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Biometrie/Gesichtserkennung_pdf.pdf?__blob=publicationFile, (29.10.2017).

[241] Vgl. *National Institute for Standardization*, https://www.nist.gov/programs-projects/face-projects, (30.10.2017).

[242] Vgl. *o. V.*, Summary of the 3D Face Project, https://www.3dface.org/project.html, (30.10.2017).

[243] Vgl. *Bundesamt für Sicherheit in der Informationstechnik*, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/BioFace/BioFaceIIBericht.pdf;jsessionid=E4ED769895DCC5E9FB946B42AC815F59.1_cid369?__blob=publicationFile&v=3, (30.10.2017).

[244] Vgl. *Bundesamt für Sicherheit in der Informationstechnik*, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/BioP/BioPI.pdf?__blob=publicationFile&v=1, (30.10.2017).

[245] Vgl. *Bundeskriminalamt*, https://www.tib.eu/de/suchen/download/?tx_tibsearch_search%5Bdocid%5D=TIBKAT%3A860865568&tx_tibsearch_search%5Bsearchspace%5D=tn&cHash=5435684b2f85792d4a1ae7a69723f683#download-mark, (30.10.2017).

[246] Vgl. *Bundesministerium für Bildung und Forschung*, https://www.sifo.de/de/ges-3d-multi-biometrische-gesichtserkennung-2103.html, (30.10.2017).

auf dem Gebiet des Lichtbildvergleiches die Möglichkeit gibt über Programme aus einem zweidimensionalen Foto dreidimensionale Köpfe oder ein Gesichtsrelief als Raumbild an einem Monitor zu gestalten. Diese Methode ist sehr anschaulich, sie ist jedoch hoch spekulativ, weshalb sie im Ermittlungsverfahren als Grundlage eines Gutachtens und mithin als Beweismittel nicht eingesetzt wird.[247] Zum anderen gab es von 2013 bis 2016 Bestrebungen Gesichtserkennung so zu verbessern, dass sie künstliche Veränderungen der Biometrie in einem menschlichen Gesicht, zum Beispiel durch Maskierungen, erkennen kann. Dieses Forschungsprojekt hieß „FeGeb: Fälschungserkennung für die Gesichtsbiometrie mit aktivem NIR Kamerasystem“ und wurde von der Hochschule Bonn-Rhein-Sieg initiiert.[248]

6 Konzeption der Analyse

Es konnte bisher dargestellt werden, dass der Beitrag der Videoüberwachung sozialwissenschaftlich, humangeografisch, juristisch und technisch gut erforscht ist. Eine kriminalistische Untersuchung, die prüft, wie erfolgreich Videoüberwachung Straftaten tatsächlich aufklärt, gibt es nicht. Wenngleich häufig zu lesen ist, dass der Videoüberwachung die Eigenschaft einer Superwaffe im Kampf gegen die Kriminalität zugeschrieben wird.[249] Die Forschungsprojekte MuVit und MisPel bezogen zumindest polizeiliche Aspekte, Ansichten und Belange mit ein, den Schwerpunkt bildeten sie jedoch nicht. Aus diesem Grund wird eine eigene empirische Untersuchung mit kriminalistischem Kernthema durchgeführt. Die Studie zu Multi-Biometriebasierter Forensischer Personensuche in Lichtbild- und Videomassendaten brachte hervor, dass die Qualität der Bilder aus Überwachungsanlagen in der polizeilichen Praxis häufig für mangelhaft befunden werden.[250] Daraus müsste eigentlich folgen, dass sie unbrauchbar für ein Ermittlungsverfahren sind oder zumindest häufig nicht (wesentlich) zum Aufklärungserfolg beitragen können. So wie bei den Ermittlungsverfahren der Silvesternacht in Köln. Dem entgegen fordern Politik und

---

[247] Vgl. *Huckenbeck et al.*, Identifikation lebender Personen anhand von Lichtbildern des Gesichts, 9.
[248] Vgl. *Bundesministerium für Bildung und Forschung*, https://www.bmbf.de/files/Projekt_des_Monats_Januar_2016.pdf, (30.10.2017); vgl. *Hochschule Bonn-Rhein-Sieg*, https://www.h-brs.de/de/fegeb, (30.10.2017).
[249] Vgl. zum Beispiel positiv über den Anteil der Videoüberwachung zur Aufklärung von Straftaten *Schnabel*, Die polizeiliche Videoüberwachung öffentlicher Orte in Niedersachsen, 879.
[250] Vgl. *Humer/Lederer*, Von der konventionellen zur intelligenten Videoüberwachung, 38.

Strafverfolgungsbehörden nach Signalereignissen trotzdem als Konsequenz immer wieder unter anderem mehr Videoüberwachung.[251] Dabei können Bilder, auf denen der Täter kaum zu erkennen ist, keinen Anspruch auf ein forensisches Beweismittel erheben und einen Beschuldigten vor Gericht nicht zweifelsfrei der Straftat überführen.

6.1 Forschungsleitfragen

Das Ziel der Analyse dieser Arbeit ist es herauszufinden, welchen Beitrag bildbasierte Ermittlungsmethoden und somit auch der Videobeweis zur Aufklärung von Straftaten leistet. Am Ende der Thesis sollen dazu folgende Forschungsleitfragen beantwortet werden können.

- Wie viele Fälle gab es im Jahr 2016, bei denen die computergestützte Gesichtserkennung, ein Lichtbildvergleich oder eine Ermittlungsöffentlichkeitsfahndung zum Einsatz kamen?
- Auf welchem Bildmaterial beruhten diese Ermittlungsmethoden?
- Wie war die Qualität des Bildmaterials?
- Wurde durch die Ermittlungsmethode ein Tatverdächtiger identifiziert?
- Wie oft lagen diesen Ermittlungserfolgen Videobeweise zugrunde?
- Werden die Täter bei gutem Bildmaterial häufiger identifiziert als bei schlechtem?
- Können die Straftaten noch aufgeklärt werden, wenn durch die bildbasierten Ermittlungsmethoden kein Tatverdächtiger ermittelt werden konnte?

6.2 Untersuchungsdesign

Zur Beantwortung der Fragen werden behördliche, statistische Daten ausgewertet, die teilweise bereits primär für interne Zwecke zusammengestellt wurden. Mithin handelt es sich bei dieser Untersuchung um eine Sekundäranalyse, welche in der politischen Arithmetik verwurzelt ist. An der Stelle, an der relevante Daten zu den Forschungsfragen fehlten, wurden die Statistiken

[251] Zum Beispiel forderte der BKA Präsident Holger Münch mehr Polizeipräsenz und Videoüberwachung nach den schlechten Ermittlungsergebnissen der Kölner Silvesternacht. Vgl. https://www.bayernkurier.de/inland/15311-viele-straftaten-bleiben-ungesuehnt/, (15.12.2017).

durch Primärerhebungen aus digitalen Verhaltensspuren ergänzt.[252] Die politische Arithmetik befasst sich mit der gesetzmäßigen quantitativen Erfassung sozialer Tatbestände.[253] Quantitative Methoden sind deduktiv, sie helfen verallgemeinerbare Aussagen durch standardisierte Datenerhebung zu produzieren.[254] Aus diesem Grund wurde eine solche für die Analyse bevorzugt. Zur Untersuchung stehen die Daten vom 01.01.2016 bis 31.12.2016, der Erfassungszeitraum beträgt 366 Tage, da es sich um ein Schaltjahr handelt. Wegen der zu erwartenden Datenmenge wird die Analyse nicht nur zeitlich, sondern auch räumlich auf den Zuständigkeitsbereich des Landes Hessen und thematisch auf die Verarbeitung der Daten der bildbasierten Ermittlungsmethoden der computergestützten Gesichtserkennung, des Lichtbildvergleiches und der Öffentlichkeitsfahndung begrenzt. Die Polizei Hessen teilt sich in die sieben folgenden Flächenpräsidien auf: Polizeipräsidium (PP) Nordhessen, PP Osthessen, PP Mittelhessen, PP Westhessen, PP Frankfurt, PP Südosthessen und PP Südhessen.[255] Die Einmaligkeit der Nutzbarmachung polizeilicher Statistiken auf diese Weise entspricht dem Charakter einer Querschnittsstudie.[256] Die auszuwertenden Daten der Polizei Hessen sind prozessproduzierte Daten im sozialwissenschaftlichen Sinne, da sie durch Arbeitsabläufe bei der Sachbearbeitung in strafrechtlichen Ermittlungsverfahren u. a. als digitale Verhaltensspuren entstanden sind.[257]

7 Methodik: Die Sekundäranalyse prozessproduzierter Daten

„Verhaltensspuren von Aktivitäten, die mit dem staatlichen Verwaltungshandeln in Verbindung stehen, werden mehr oder minder systematisch (…) erfasst. (…) Auch private Archive und Registraturen (…) stellen häufig aufschlussreiche Datenquellen für (…) Untersuchungen dar.“[258] Die Sekundäranalyse nimmt zur Beantwortung von Forschungsleitfragen gern bereits vorhandene Daten zur Hilfe. Sie ist keine klassische Erhebungsmethode, sie nutzt vielmehr eine existierende, bereits erhobene, Datenbasis. Diese Daten bzw.

[252] Vgl. *Diekmann*, Empirische Sozialforschung, 92.
[253] Vgl. *Diekmann*, Empirische Sozialforschung, 94f.
[254] Vgl. *Häder*, Empirische Sozialforschung, 13.
[255] Vgl. Die Behörden und Einrichtungen der Polizei Hessen, https://www.polizei.hessen.de/Dienststellen/, (04.11.2017).
[256] Vgl. *Häder*, Empirische Sozialforschung, 112.
[257] Vgl. *Diekmann*, Empirische Sozialforschung, 652f.
[258] *Diekmann*, Empirische Sozialforschung, 653.

Datenbasen sind in der Regel nicht aufbereitet und nicht interpretiert.[259] Man spricht von passivem nichtreaktivem Material.[260] Da eine Sekundäranalyse eben keine eigene Erhebungsmethode besitzt, kann an dieser Stelle keine spezifische Verfahrensweise erläutert werden.[261] Der Vorteil einer Sekundäranalyse ist, dass sie durch den Rückgriff auf statistische Datensätze eine gezielte, problemorientierte Analyse ermöglicht.[262] Ihr Ziel ist es, wie bei der Primäranalyse auch, neue Erkenntnisse hervorzubringen.[263] Die Umsetzung der Sekundäranalyse lässt sich für die ausgewählten Ermittlungsmethoden im Einzelnen aus den folgenden Unterkapiteln entnehmen.

7.1 Umsetzung der Methodik bei GES und Lichtbildvergleich

Die Datenbasis der Fälle computergestützter Gesichtserkennung und Lichtbildvergleiche bildet eine statistische Erhebung des Hessischen Landeskriminalamtes für das Jahr 2016. Die Datenquelle ist somit der amtliche Speicher einer Behörde. Jeder Untersuchungsantrag auf Gesichtserkennung und Lichtbildvergleich entspricht einer Untersuchungseinheit, also einem Fall. Für jede Untersuchungseinheit wurden zielgerichtet folgende Variablen bestimmt:

- Herkunft
- Bildmaterial
- Qualität des Bildmaterials
- Urteil
- Identifizierung
- Aufklärung der Straftat

Die Variablen *Herkunft, Urteil* und *Identifizierung* konnten ohne Weiteres aus der Statistik übernommen werden. Die Variablen *Bildmaterial*, *Qualität des Bildmaterials* und *Aufklärung der Straftat* wurden aus digitalen Verhaltensspuren, den Expertengutachten sowie aus dem hessischen Index für computer-

[259] Vgl. *Medjedovic*, Qualitative Sekundäranalyse, 20.
[260] Vgl. *Diekmann*, Empirische Sozialforschung, 653.
[261] Vgl. *Medjedovic*, Qualitative Sekundäranalyse, 26.
[262] Vgl. *Medjedovic*, Qualitative Sekundäranalyse, 40.
[263] Vgl. *Medjedovic*, Qualitative Sekundäranalyse, 23.

gestützte Vorgangsbearbeitung entnommen und ergänzt. Die Variablen wurden wie folgt polytom kategorisiert, bzw. sind wie folgt dichotom ausgeprägt.[264] Die Variable *Herkunft* beinhaltet die Kategorien PP Nordhessen (PPNH), PP Osthessen (PPOH), PP Mittelhessen (PPMH), PP Westhessen (PPWH), PP Frankfurt (PPFFM), PP Südosthessen (PPSOH), PP Südhessen (PPSH), das Hessische Landeskriminalamt (HLKA), Gerichte, Staatsanwaltschaften und den Zoll. Die Kategorien umfassen alle potenziellen Antragssteller. Die Variable *Bildmaterial* setzt sich aus den Kategorien Passbild, Videoüberwachung privat (private Institution), Videoüberwachung staatlich, Videoüberwachung Privatperson, Privataufnahme (z. B. Fotos, Profilbilder), Lichtbild aus Geschwindigkeitsüberwachungsanlage und Polizeifoto (z. B. Bilder aus einer erkennungsdienstlichen Behandlung) zusammen. Die *Qualität des Bildmaterials* wurde dichotom in gut und schlecht eingeteilt. Dabei wurden die Bilder nach ihrer Pixelgröße beurteilt und für gut befunden, wenn Individualmerkmale der Person zur zweifelsfreien Identifizierung erkennbar waren. Als schlecht wurde das Bildmaterial erwogen, wenn dies nicht der Fall war und ein Lichtbild Störfaktoren aufwies. Hierzu wurden zur Objektivierung das zugrunde liegende Bildmaterial sowie die dazugehörigen Expertengutachten gesichtet. Die Variable *Identifizierung* wurde für die Ermittlungsmethode der computergestützten Gesichtserkennung ebenfalls dichotom in ja und nein eingeteilt. Die Variable *Urteil* enthält hier die Kategorien Treffer, kein Treffer und nicht auswertbar. Gab es einen Treffer mit registriertem Bildmaterial aus der Referenzdatenbank, dann wurde die Person identifiziert, gab es keinen Treffer wurde, sie nicht identifiziert.

Für die Ermittlungsmethode des Lichtbildvergleiches muss aufgrund der in Kapitel 3.3 erwähnten abgestuften Identifizierungsprädikate differenzierter vorgegangen werden. Die vergebenen Prädikate sind in den elf Kategorien beschrieben und durch die Variable *Urteil* abgebildet. Eine *Identifizierung* des Täters wurde bei den Prädikaten „mit an Sicherheit grenzender Wahrscheinlichkeit“ (maSgW), „mit hoher Wahrscheinlichkeit“ (mhW) und „wahrscheinlich“ (W) angenommen. Für die Prädikate „es deutet daraufhin, dass es sich um ein und dieselbe Person handelt“, „es kann nicht ausgeschlossen werden, dass

[264] Vgl. zur Erläuterung der Ausprägungen einer Variable in dichotom und polytom auch *Diekmann*, Empirische Sozialforschung, 118.

es sich um ein und dieselbe Person handelt“ wurde eine schwache Identifizierung angenommen. Bei den Prädikaten „mit an Sicherheit grenzender Wahrscheinlichkeit ist eine Identität nicht gegeben“ (maSgW nicht), „mit hoher Wahrscheinlichkeit ist eine Identität nicht gegeben“ (mhW nicht), „wahrscheinlich ist Identität nicht gegeben“ (W nicht) wurde eine eindeutige Nichtidentifizierung und Entlastung eines Tatverdächtigen kategorisiert. Bei einer Beurteilung mit „es deutet darauf hin, dass es sich nicht um ein und dieselbe Person handelt“, „es kann nicht ausgeschlossen werden, dass es sich nicht um ein und dieselbe Person handelt“ wurde eine schwach negative Identifizierung angenommen. Bei den Aussagen „es kann weder bestätigt noch ausgeschlossen werden, dass es sich um ein und dieselbe Person handelt“ sowie die Prädikate „nicht auswertbar“ und „ohne Prädikat“ wurde kein identifizierendes Werturteil angenommen, diesem wurde mit der Kategorie „ohne Angaben“ Rechnung getragen.

Die Variable *Aufklärung der Straftat* bezieht sich wiederum für beide Ermittlungsmethoden gleich darauf, ob die Straftat letztlich (trotzdem) aufgeklärt wurde. Wurde ein Tatverdächtiger als Beschuldigter im Ermittlungsverfahren eingetragen, dann gilt die Tat im statistischen Sinne als geklärt (ja). Wurde der Täter nicht identifiziert und wurde kein Beschuldigter im Ermittlungsverfahren eingetragen, gilt die Straftat in dieser Untersuchung als nicht geklärt (nein).[265] Alle Variablen und Kategorien wurden in das Statistikprogramm SPSS übertragen und mit der Software ausgewertet sowie verbildlicht.

7.2 Hypothesen zur GES und dem Lichtbildvergleich

Die nunmehr mit dem Datenmaterial zu überprüfenden Hypothesen lauten im Sinne der Forschungsleitfragen:

- Computergestützte Gesichtserkennung/ Lichtbildvergleiche beruhen öfter auf Bildern aus Videoüberwachungsanlagen als auf Bildern anderer Quellen.

[265] Vgl. zum Begriff <Aufgeklärte Straftaten> die Richtlinien für die Führung der *Polizeilichen Kriminalstatistik (PKS)* i. d. F. vom 01.01.2016, https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/PolizeilicheKriminalstatistik/2016/pks2016Richtlinien.html, 5, (11.11.2017).

- Die Bildqualität der Aufnahmen aus Videoüberwachungsanlagen ist überwiegend schlecht.
- Computergestützte Gesichtserkennung und Lichtbildvergleiche tragen erheblich zur Identifizierung von Straftätern bei.
- Videoüberwachung trägt öfter zur Identifizierung von Straftätern bei als andere Bildquellen.
- Straftäter werden durch computergestützte Gesichtserkennung/ Lichtbildvergleiche öfter bei guter Bildqualität identifiziert.
- Computergestützte Gesichtserkennung und Lichtbildvergleiche tragen erheblich zur Aufklärung von Straftaten bei.

7.3 Umsetzung der Methodik bei der Öffentlichkeitsfahndung

Die Datenbasis der Fälle von Öffentlichkeitsfahndungen bildeten digitale Verhaltensspuren der Sachbearbeiter im Internet. Es gibt landesweit keine anterograde statistische Erhebung zur Anzahl und Ausprägung von Öffentlichkeitsfahndungen. Die Entscheidung darüber, ob eine Öffentlichkeitsfahndung die Ermittlungen in einer Strafsache voranbringen kann, wird meistens auf Sachbearbeiter Ebene getroffen und von dort aus an die Staatsanwaltschaft herangetragen. Öffentlichkeitsfahndungen ergehen daher dezentral und lokal, ohne Registrierung in einem allgemeinen Erfassungsinstrument. Die Öffentlichkeitsfahndungen werden durch die Flächenpräsidien an das Presseportal weitergegeben. Unter der Rubrik Blaulichtmeldungen mit Bild konnten alle Öffentlichkeitsfahndungen der einzelnen Polizeidirektionen, ergo der Flächenpräsidien des Landes Hessen für den Bezugszeitraum retrograd nachvollzogen und erfasst werden. [266] Wie bereits zuvor erwähnt, beschränkt sich die Untersuchung auf Ermittlungsöffentlichkeitsfahndungen gem. § 131 b StPO. Diese wurden aus den digital einsehbaren Fahndungen selektiert und folgende Variablen pro Fall bestimmt:

- Herkunft
- Bildmaterial

[266] http://www.presseportal.de/, (12.11.2017).

- Qualität des Bildmaterials
- Identifizierung
- Aufklärung der Straftat.

Jede Öffentlichkeitsfahndung entspricht einer Untersuchungseinheit. Wenn in einem Fall nach zwei unbekannten Tätern gefahndet wurde, so wurde dies in diesem Zusammenhang als eine Öffentlichkeitsfahndung gewertet. Wie auch bei den Gesichtserkennungsverfahren, teilt sich die Variable *Herkunft* in die sieben Flächenpräsidien auf. Die Variable *Bildmaterial* besteht aus den Kategorien Phantombild, Privataufnahme, Videoüberwachung privat, Videoüberwachung staatlich und Videoüberwachung Privatperson. Die *Qualität des Bildmaterials* wurde wieder wie bei den Gesichtserkennungsverfahren bestimmt. Sofern der Fahndung digitales Bildmaterial aus (Video)Kameras vorlag, wurden die Bilder bei geringer Pixelgröße und Erkennbarkeit von Individualmerkmalen für gut und andernfalls für schlecht befunden. Ein Phantombild wurde immer als gut bewertet, da es grundsätzlich auf den Merkmalen eines Tatverdächtigen mit Wiedererkennungswert beruht, die von einem Zeugen wiedergegeben werden.[267] Bei der Öffentlichkeitsfahndung kann im Hinblick auf die Variable *Identifizierung* nur eine verlässliche Aussage darüber getroffen werden, wie viele der Ermittlungsöffentlichkeitsfahndungen nicht zur Identifizierung eines Tatverdächtigen führten. Es kann anhand der Datenbasis retrograd keine valide Aussage darüber getroffen werden, ob bei den aufgeklärten Fällen, der Täter durch die Fahndung oder auf andere Weise ermittelt wurde. Hierzu wäre eine Befragung der einzelnen Sachbearbeiter notwendig gewesen, was nicht Bestandteil der Genehmigung war. Für die Variable *Aufklärung der Straftat* gilt hingegen wieder: Wurde ein Beschuldigter im Ermittlungsverfahren eingetragen, dann ist die Straftat im statistischen Sinne geklärt, wurde kein Beschuldigter eingetragen, dann blieb die Straftat ungeklärt. Zur Erhebung dieser Kategorien wurden über polizeiliche Lagebilder die Vorgangsnummern recherchiert und damit der Beschuldigtenstatus über den Index der computergestützten Vorgangsbearbeitung ermittelt. Alle Variablen und Kategorien

[267] Vgl. *Averdiek-Gröner/Frings*, Standardmaßnahmen im Ermittlungsverfahren, 128f.

wurden ebenfalls in das Statistikprogramm SPSS übertragen und mit der Software ausgewertet und verbildlicht.

7.4 Hypothesen zur Öffentlichkeitsfahndung

Die nunmehr mit dem Datenmaterial zu überprüfenden Hypothesen lauten im Sinne der Forschungsleitfragen wie bei dem Abschnitt Gesichtserkennung:

- Ermittlungsöffentlichkeitsfahndungen beruhen öfter auf Bildern aus Videoüberwachungsanlagen als auf Bildern anderer Quellen.
- Die Bildqualität der Aufnahmen aus Videoüberwachungsanlagen ist überwiegend schlecht.
- Ermittlungsöffentlichkeitsfahndung trägt erheblich zur Identifizierung von Straftätern bei.
- Videoüberwachung trägt dabei öfter zur Identifizierung von Straftätern bei als andere Bildquellen.
- Straftäter werden durch Ermittlungsöffentlichkeitsfahndung öfter bei guter Bildqualität identifiziert.
- Ermittlungsöffentlichkeitsfahndung trägt erheblich zur Aufklärung von Straftaten bei.

8 Untersuchungsergebnisse der Gesichtserkennung

In Hessen gab es im Bezugszeitraum 2016 insgesamt 256 Fälle computergestützter Gesichtserkennung und Lichtbildvergleiche. Es wurden 106 Gutachten zu Untersuchungsaufträgen auf computergestützte Gesichtserkennung und 150 Gutachten zu Lichtbildvergleichen gefertigt. Es gab acht unspezifische Anfragen an das zuständige Sachgebiet des HLKA, die unberücksichtigt bleiben. Nach weiterem Abzug der Untersuchungseinheiten, denen keine Straftat zugrunde lag, um deren Aufklärung es ging oder die zurückgezogen wurden, verbleiben für die Auswertung 104 Lichtbildvergleiche und 101 Fall computergestützter Gesichtserkennung.

8.1 Ergebnisse der computergestützten Gesichtserkennung

Die 101 Fälle computergestützter Gesichtserkennung verteilen sich in Hessen auf folgende Untersuchungsantragsteller.

Das zuständige Sachgebiet des HLKA wurde in 30 Fällen durch das PPFFM um computergestützte Gesichtserkennung ersucht. Das PPMH folgt mit insgesamt 22 Anträgen. Das PPSH hatte 16 Anfragen auf computergestützte Gesichtserkennung, das PPSOH 14 und das PPWH elf. Etwas weniger Fälle verteilen sich auf das PPNH mit fünf und das PPOH mit zwei Untersuchungseinheiten. Der Zoll forderte als externe Behörde in einem Falle ein Gutachten zur computergestützten Gesichtserkennung an, siehe *Abbildung 3*.

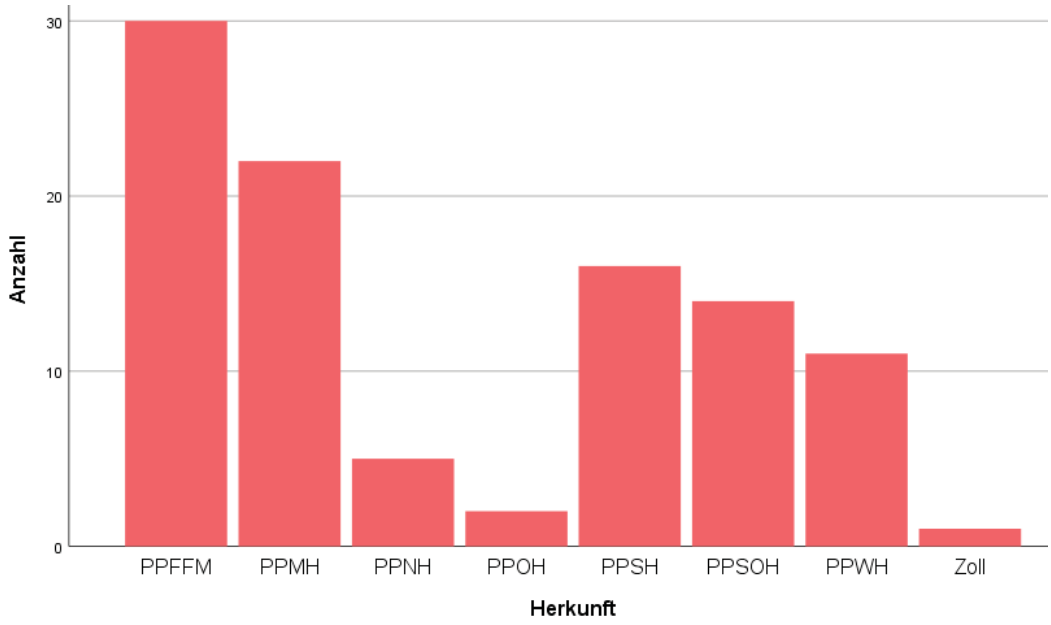

Abbildung 3: Verteilung der computergestützten Gesichtserkennung in Hessen

Forschungshypothese 1: *Computergestützte Gesichtserkennung beruht öfter auf Bildern aus Videoüberwachungsanlagen als auf Bildern anderer Quellen*.

37 Untersuchungseinheiten (36,6 %) beruhten auf dem Abgleich von Passbildern mit der polizeilichen Referenzdatenbank für erkennungsdienstlich behandelte Straftäter. 28 Untersuchungseinheiten hatten Privataufnahmen zur Grundlage (27,7 %). In 23 Fällen wurde Videoüberwachungsmaterial privater

Institutionen abgeglichen (22,8 %) und in sechs Fällen Videoüberwachungsmaterial von Privatpersonen (5,9 %). Der Anteil von Videoüberwachungsmaterial beträgt somit insgesamt 28,7 %, siehe *Tabelle 1*.

Bildmaterial

		Häufigkeit	Prozent	Gültige Prozente	Kumulierte Prozente
Gültig	ED Bild	3	3,0	3,0	3,0
	Lichtbild Geschwindigkeitsüberwachungsanlage	4	4,0	4,0	6,9
	Passbild	37	36,6	36,6	43,6
	Privataufnahme	28	27,7	27,7	71,3
	Videoüberwachung privat	23	22,8	22,8	94,1
	Videoüberwachung Privatperson	6	5,9	5,9	100,0
	Gesamt	101	100,0	100,0	

Tabelle 1: Aufschlüsselung des Bildmaterials (GES)

Die Forschungshypothese wurde somit widerlegt. Computergestützte Gesichtserkennung beruht in den meisten Fällen auf Passbildern und nicht auf Bildern aus Videoüberwachungsanlagen.

Forschungshypothese 2: *Die Bildqualität der Aufnahmen aus Videoüberwachungsanlagen ist überwiegend schlecht*.
Es gab insgesamt 29 Untersuchungseinheiten, die auf Bildern aus Videoüberwachungsanlagen und 72 Untersuchungseinheiten, die auf anderen Bildquellen beruhten. Von den 29 Untersuchungseinheiten mit Bildmaterial aus Videoüberwachungsanlagen, hatten 25 schlechtes Bildmaterial und nur vier gutes. Bei den übrigen Bildquellen stellt sich das Verhältnis kumulativ umgekehrt dar. 46 Bilder waren guter und 26 schlechter Qualität.
Die Bilder aus erkennungsdienstlichen Behandlungen sind guter Qualität. Drei Bilder aus Geschwindigkeitsüberwachungsanlagen waren schlecht, nur eins gut. 25 von 28 Privataufnahmen hatten eine gute Bildqualität, drei eine schlechte. Bei den Passbildern ergab sich ein Verhältnis von 17:20. 17 Bilder waren gut und 20 schlecht, *siehe Abbildung 4*. Dieses Verhältnis kommt daher, dass viele Passbilder nicht in ihrer digitalen Originalform, sondern als Kopie vorlagen, oder sogar nur als gescannt/kopierte Kopie.

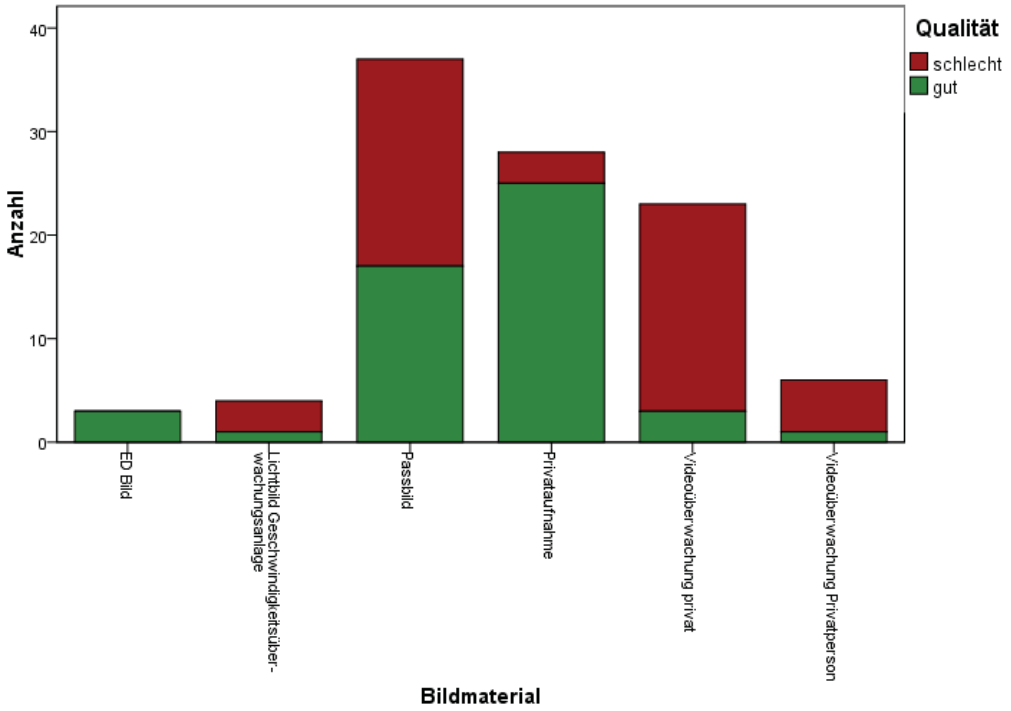

Abbildung 4: Qualitätsverteilung aller Bildquellen (GES)

Im Ergebnis ist ersichtlich, dass das Bildmaterial aus Videoüberwachungsanlagen überwiegend schlecht ist. Die Forschungshypothese wurde bestätigt.

Forschungshypothese 3: *Computergestützte Gesichtserkennung trägt erheblich zur Identifizierung von Straftätern bei*.
In 90 Fällen (89,1 %) konnte die Software keinen Tatverdächtigen identifizieren. In elf Untersuchungseinheiten konnte sie entsprechende Personalien zu einem bislang unbekannten Tatverdächtigen liefern (10,9 %), siehe *Tabelle 2*.

Identifizierung

		Häufigkeit	Prozent	Gültige Prozente	Kumulierte Prozente
Gültig	nein	90	89,1	89,1	89,1
	ja	11	10,9	10,9	100,0
	Gesamt	101	100,0	100,0	

Tabelle 2: Identifizierung von Tatverdächtigen (GES)

Die Forschungshypothese kann daher nicht bestätigt werden, computergestützte Gesichtserkennung trägt nicht erheblich zur Identifizierung von Straftätern bei.

Forschungshypothese 4: *Videoüberwachung trägt dabei öfter zur Identifizierung von Straftätern bei als andere Bildquellen*.
Keine der elf Identifizierungen beruhte auf Videoüberwachungsmaterial.
Die elf Identifizierungen erfolgten auf Basis der Bildmaterialien ED Bild (2), Passbild (5) und Privataufnahme (4), *siehe Tabelle 3*.

Bildmaterial * Identifizierung Kreuztabelle

Anzahl

		Identifizierung		
		nein	ja	Gesamt
Bildmaterial	ED Bild	1	2	3
	Lichtbild Geschwindigkeitsüberwachungsanlage	4	0	4
	Passbild	32	5	37
	Privataufnahme	24	4	28
	Videoüberwachung privat	23	0	23
	Videoüberwachung Privatperson	6	0	6
Gesamt		90	11	101

Tabelle 3: Aufschlüsselung Identifizierung/ Bildbasis (GES)

Videoüberwachung trägt nicht öfter zur Identifizierung von Straftätern durch computergestützte Gesichtserkennung bei. Die Forschungshypothese wurde widerlegt.

Forschungshypothese 5: *Straftäter werden mit computergestützter Gesichtserkennung bei guter Bildqualität öfter identifiziert*.
Die Auswertung hat ergeben, dass zwei Bilder, trotz schlechter Qualität, mit der Gesichtserkennungssoftware zur Identifizierung eines Tatverdächtigen führen konnte. Neun der identifizierten Tatverdächtigen, lag gutes Bildmaterial zugrunde, siehe *Tabelle 4*. Bisher könnte man der Forschungshypothese zustimmen.

Qualität * Identifizierung Kreuztabelle

Anzahl

		Identifizierung		
		nein	ja	Gesamt
Qualität	schlecht	49	2	51
	gut	41	9	50
Gesamt		90	11	101

Tabelle 4: Verhältnis der Bildqualität zur Täteridentifizierung (GES)

Es zeichnet sich jedoch außerdem ab, dass sich das Verhältnis schlechter und guter Qualität mit 51:50 in etwa die Waage hält. Insgesamt 41 Lichtbilder, brachten trotz guter Qualität, keinen Tatverdächtigen hervor. Das liegt daran, dass die Täter zuvor nicht erkennungsdienstlich behandelt waren und zeigt, dass die Wahrscheinlichkeit einer Identifizierung nicht nur von der Bildqualität, sondern auch vom Umfang der Referenzdatenbank abhängig ist. Straftäter werden nicht zwangsläufig bei guter Bildqualität mit computergestützter Gesichtserkennung öfter identifiziert. Die Forschungshypothese ist nur bedingt richtig.

Forschungshypothese 6: *Computergestützte Gesichtserkennung trägt erheblich zur Aufklärung von Straftaten bei*.
Alle elf Treffer der computergestützten Gesichtserkennung führten zur Aufklärung der Straftaten. In den 90 Fällen, die nicht über die Gesichtserkennungssoftware geklärt werden konnten, wurde in 46 Fällen auf andere Art und Weise ein Beschuldigter ermittelt, siehe *Tabelle 5*.

Identifizierung * Aufklärung Kreuztabelle

Anzahl

		Aufklärung			
		nein	ja	unbekannt	Gesamt
Identifizierung	nein	41	46	3	90
	ja	0	11	0	11
Gesamt		41	57	3	101

Tabelle 5: Aufklärung der Straftaten (GES)

Die Forschungshypothese ist widerlegt.

8.2 Ergebnisse der Lichtbildvergleiche

Die 104 Fälle der Lichtbildvergleiche verteilten sich in Hessen auf folgende Untersuchungsantragsteller.

Das HLKA wurde zweimal durch hessische Gerichte und einmal durch eine hessische Staatsanwaltschaft beauftragt, einen Lichtbildvergleich durchzuführen. Das Polizeipräsidium Frankfurt am Main und das Polizeipräsidium Mittelhessen hatten jeweils 19 Untersuchungsaufträge auf Lichtbildvergleiche. Ihnen folgt das Polizeipräsidium Westhessen mit 14 Lichtbildvergleichen. Das Polizeipräsidium Südhessen hatte 13 Lichtbildvergleiche in 2016 und die Polizeipräsidien Nordhessen, Osthessen und Südosthessen jeweils zehn. Durch das HLKA selber wurden sechs Lichtbildvergleiche beauftragt, siehe *Abbildung 5*.

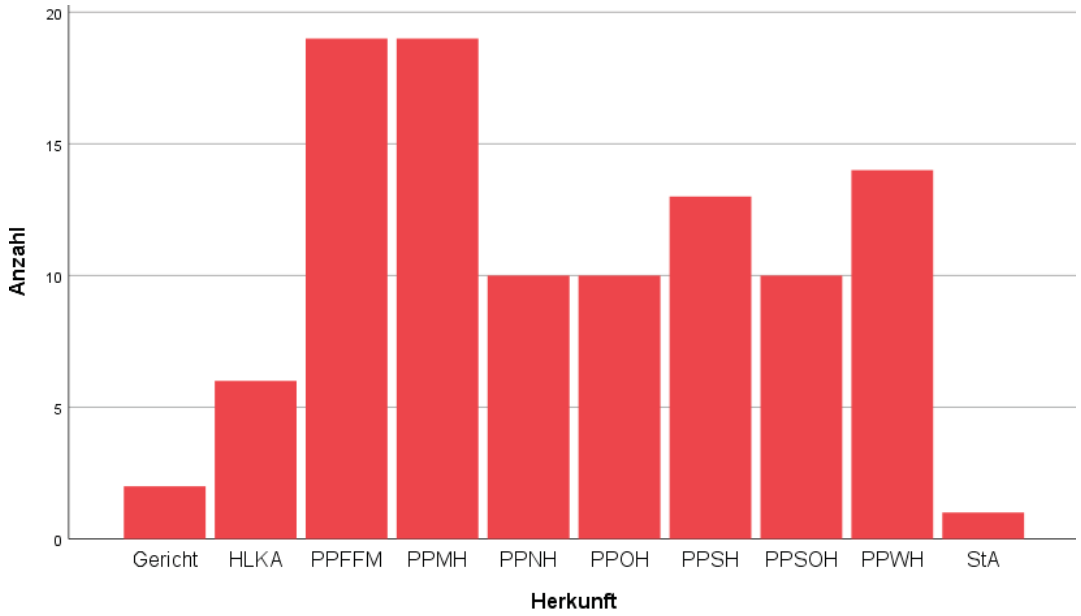

Abbildung 5: Verteilung der Lichtbildvergleiche in Hessen

Forschungshypothese 1: *Lichtbildvergleiche beruhen öfter auf Bildern aus Videoüberwachungsanlagen als auf Bildern anderer Quellen*.

Bei 58,6 % der Lichtbildvergleiche bestand das Vergleichsmaterial aus Videoüberwachungsanlagen vom Tatort. Hierbei wurde zunächst nicht zwischen staatlicher und privater Videoüberwachung durch Institutionen sowie Privatpersonen unterschieden. Als wichtige Bildbasis mit 17,3 % stellen sich neben der Videoüberwachung die Passbilder und mit 11,5 % die Privataufnahmen

dar. Die mit Abstand meisten Bilder liefern Videoüberwachungsanlagen privater Institutionen (51,9 %), siehe *Tabelle 6*.

Bildmaterial

		Häufigkeit	Prozent	Gültige Prozente	Kumulierte Prozente
Gültig	Lichtbild Geschwindigkeitsüberwachungsanlage	10	9,6	9,6	9,6
	Passbild	18	17,3	17,3	26,9
	Polizeifoto	3	2,9	2,9	29,8
	Privataufnahme	12	11,5	11,5	41,3
	Videoüberwachung privat	54	51,9	51,9	93,3
	Videoüberwachung Privatperson	5	4,8	4,8	98,1
	Videoüberwachung staatlich	2	1,9	1,9	100,0
	Gesamt	104	100,0	100,0	

Tabelle 6: Aufschlüsselung des Bildmaterials (LV)

Im Ergebnis kann die Forschungshypothese bestätigt werden. Lichtbildvergleiche beruhen zu einem hohen Prozentsatz auf Bildern aus Videoüberwachungsanlagen.

Forschungshypothese 2: *Die Bildqualität der Aufnahmen aus Videoüberwachungsanlagen ist überwiegend schlecht*.
61 Untersuchungseinheiten beruhten auf Videoüberwachungsmaterial, 43 auf anderen Bildquellen. In 56 von 61 Untersuchungseinheiten, war die Qualität des Bildmaterials schlecht. Fünf Bilder waren guter Qualität. Bei der Qualität der anderen Bildquellen ist das Verhältnis kumulativ umgekehrt. Von 43 Fällen waren 16 schlechter Bildqualität und 27 guter.
Das Bildmaterial aus den Kategorien Passbild, Polizeifoto und Privataufnahme, welches mit Fotokameras gefertigt wurde, ist überwiegend gut. Die Qualität von Lichtbildern aus Geschwindigkeitsüberwachungsanlagen ist mit einem Verhältnis von 3:7 eher schlecht, siehe *Abbildung 6*.

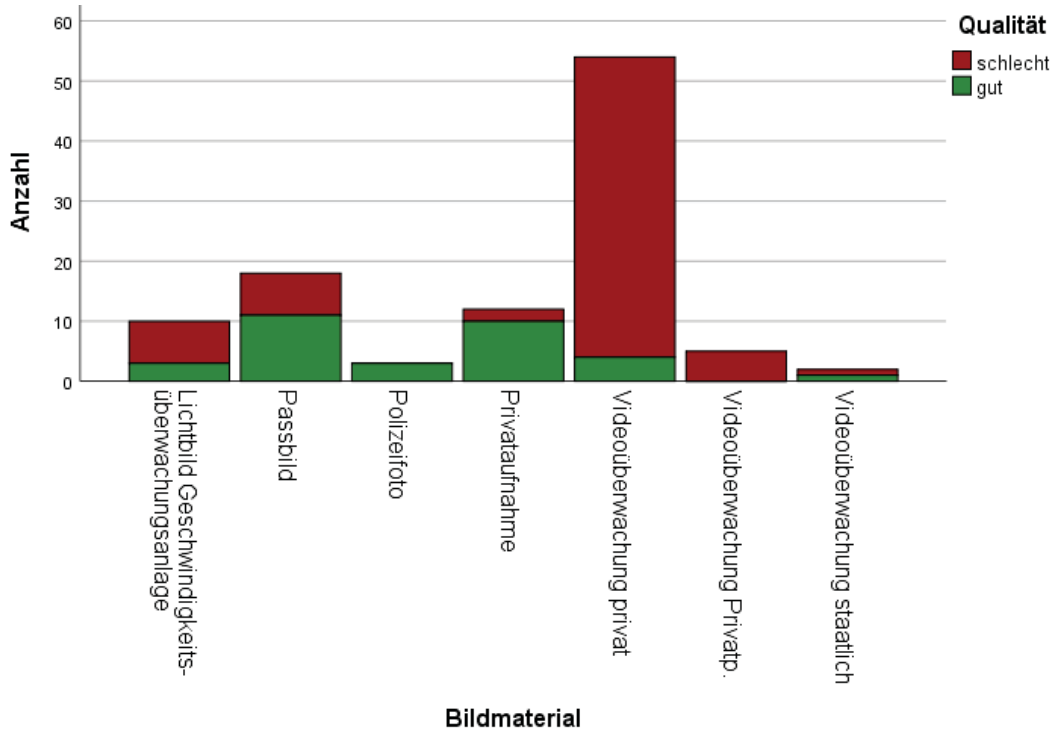

Abbildung 6: Qualitätsverteilung aller Bildquellen (LV)

Die Forschungshypothese, dass Videobeweise überwiegend eine schlechte Bildqualität haben, konnte bestätigt werden.

Forschungshypothese 3: *Lichtbildvergleiche tragen erheblich zur Identifizierung von Straftätern bei*.

In 19 der 104 Fälle (18,3 %) konnte kein Urteil mit Tendenz vergeben werden. In zehn Fällen (9,6 %) konnte nicht ausgeschlossen werden, dass es sich bei dem Tatverdächtigen und dem Täter um ein- und dieselbe Person handelt. Bei zwölf Untersuchungseinheiten deutete es daraufhin (11,5 %) und bei elf (10,6 %) war es wahrscheinlich, dass es sich bei einem Tatverdächtigen um den Täter handelt. In sechs Fällen (5,8 %) lag eine hohe Wahrscheinlichkeit der Täterschaft vor, in elf Fällen (10,6) wurde die Täterschaft mit an Sicherheit grenzender Wahrscheinlichkeit beurteilt. In einem Fall (1,0 %) konnte mit an Sicherheit grenzender Wahrscheinlichkeit eine Täterschaft ausgeschlossen werden, in sechs Fällen (5,8 %) mit hoher Wahrscheinlichkeit und in sieben (6,7 %) wahrscheinlich. In 17 Fällen (16,3 %) deutete es daraufhin, dass es sich bei dem Tatverdächtigen nicht um den Täter handelt und in vier Fällen

(3,8 %) konnte nicht ausgeschlossen werden, dass es sich bei dem Tatverdächtigen und dem Täter nicht um ein- und dieselbe Person handelt, siehe *Tabelle 7*.

Urteil

		Häufigkeit	Prozent	Gültige Prozente	Kumulierte Prozente
Gültig	Ohne Identifizierung	19	18,3	18,3	18,3
	nicht ausgeschlossen	10	9,6	9,6	27,9
	deutet hin	12	11,5	11,5	39,4
	W	11	10,6	10,6	50,0
	mhW	6	5,8	5,8	55,8
	maSgW	11	10,6	10,6	66,3
	nicht ausgeschlossen, dass nicht	4	3,8	3,8	70,2
	deutet nicht hin	17	16,3	16,3	86,5
	W nicht	7	6,7	6,7	93,3
	mhW nicht	6	5,8	5,8	99,0
	maSgW nicht	1	1,0	1,0	100,0
	Gesamt	104	100,0	100,0	

Tabelle 7: Häufigkeitsverteilung der Prädikate (LV)

Für eine Identifizierung bzw. Nichtidentifizierung des Täters sprechen die starken Prädikate mit an Sicherheit grenzender Wahrscheinlichkeit (maSgW), mit hoher Wahrscheinlichkeit (mhW) und wahrscheinlich (W). Bei den Prädikaten es deutet daraufhin und es kann nicht ausgeschlossen werden, liegt eine schwache Identifizierung bzw. Nichtidentifizierung vor.

Das würde bedeuten, dass mithilfe des Lichtbildvergleiches in 14 Fällen (13,5 %) eine Täterschaft ausgeschlossen und in 28 Fällen (26,9 %) eine Täterschaft verifiziert werden konnte. Zusammen sind das 40,4 % der Lichtbildvergleiche. In 22 Fällen (21,2 %) ging die Tendenz dahin, dass es sich bei dem Tatverdächtigen um den Täter handelt und in 21 Fällen (20,2 %) tendierten die Gutachter dazu, dass es sich bei einem Tatverdächtigen nicht um den Täter handelt, siehe *Tabelle 8*.

Identifizierung

		Häufigkeit	Prozent	Gültige Prozente	Kumulierte Prozente
Gültig	Nichtidentifizierung	14	13,5	13,5	13,5
	Identifizierung	28	26,9	26,9	40,4
	schwach positiv	22	21,2	21,2	61,5
	schwach negativ	21	20,2	20,2	81,7
	ohne Angabe	19	18,3	18,3	100,0
	Gesamt	104	100,0	100,0	

Tabelle 8: Häufigkeitsverteilung der Identifizierung von Tatverdächtigen (LV)

Lichtbildvergleiche tragen zwar nicht erheblich zur Identifizierung eines Täters oder zur Verifizierung einer Täterschaft bei, aber sie sind geeignet im Zweifel mindestens eine Tendenz zu bestimmen.

Forschungshypothese 4: *Videoüberwachung trägt dabei öfter zur Identifizierung von Straftätern bei als andere Bildquellen*.
In neun von 61 Lichtbildvergleichen (14,8 %) mit Material aus Videoüberwachungsanlagen konnte (relativ) sicher eine Täterschaft belegt werden. Bei den anderen Bildquellen waren es 19 (relativ) sichere Identifizierungen bei 43 Lichtbildvergleichen (44,2 %). Durch Videoüberwachungsanlagen konnten vier Tatverdächtige (relativ) sicher ausgeschlossen werden (6,6 % der Lichtbildvergleiche aus Videoüberwachung), durch andere Bildquellen konnten 10 Tatverdächtige als Täter ausgeschlossen werden (23,3 % der Lichtbildvergleiche mit Bildmaterial aus anderen Quellen), siehe *Abbildung 7*.
Es zeigt sich mithin insgesamt, dass auf Basis von Videoüberwachungsmaterial im Gegensatz zur Basis von Fotomaterial aus anderen Bildquellen weniger eindeutige und sichere Prädikate vergeben werden, sowohl absolut als auch prozentual. Die Zahl der unsicheren Prädikate und hier dargestellten schwachen Identifizierungen (schwach positiv) bzw. Nichtidentifizierungen (schwach negativ) sowie die Zahl der Fälle, in denen keine (Aus-)Wertung vorgenommen werden konnte, ist bei der Videoüberwachung hingegen höher als bei anderen Bildquellen.

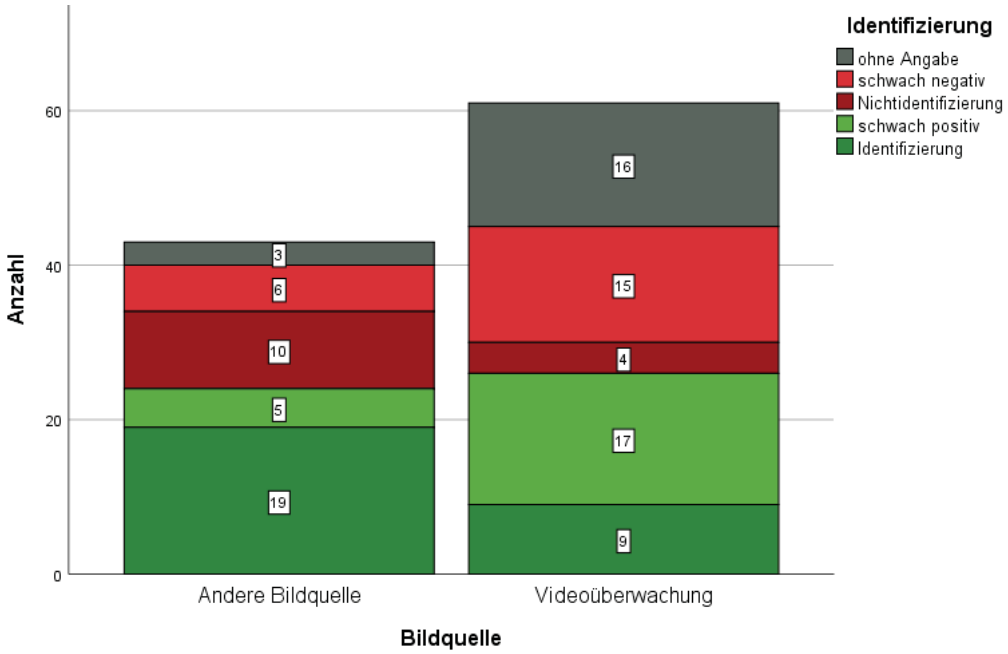

Abbildung 7: Identifizierung von Straftätern durch Videoüberwachung (LV)

Die Forschungshypothese wurde im Ergebnis nicht bestätigt.

Forschungshypothese 5: *Straftäter werden durch Lichtbildvergleiche bei guter Bildqualität öfter identifiziert*.

72 Untersuchungseinheiten beruhten auf schlechtem Bildmaterial (69,2 %) und 32 Untersuchungseinheiten besaßen gut verwertbares Bildmaterial (30,8 %).

Im Falle guter Bildqualität konnten 19 (relativ) sichere Identifizierungen und 8 (relativ) sichere Nichtidentifizierungen bekundet werden. Das heißt, in insgesamt 27 der 32 Untersuchungseinheiten mit gut verwertbarem Bildmaterial konnte ein aussagekräftiges Prädikat vergeben werden (84,4 % der Fälle mit guter Bildqualität). Bei schlechter Bildqualität konnten neun (relativ) sichere Identifizierungen und sechs (relativ) sichere Nichtidentifizierungen ausgesagt werden. Das heißt, dass in nur insgesamt 15 der 72 Fälle schlechter Bildqualität ein aussagekräftiges Prädikat verteilt werden konnte (20,8 % der Fälle mit schlechter Bildbasis). Bei schlechter Bildqualität überwiegen die schwachen Prädikate mit insgesamt 54,2 % aller schlechten Bilder. In 18 Untersuchungseinheiten konnte sogar gar kein wertendes Urteil abgegeben werden, siehe *Tabelle 9*.

Qualität * Identifizierung Kreuztabelle

Anzahl

		Identifizierung					
		Nichtidentifizierung	Identifizierung	schwach positiv	schwach negativ	ohne Angabe	Gesamt
Qualität	schlecht	6	9	20	19	18	72
	gut	8	19	2	2	1	32
Gesamt		14	28	22	21	19	104

Tabelle 9: Verhältnis der Bildqualität zur Täteridentifizierung (LV)

Die Forschungshypothese konnte verifiziert werden. Straftäter werden eher bei guter Bildqualität identifiziert.

Forschungshypothese 6: *Lichtbildvergleiche tragen erheblich zur Aufklärung von Straftaten bei*.

Die Fälle mit stark identifizierendem Prädikat wurden nachvollziehbar durch die Lichtbildvergleiche aufgeklärt. In den 14 Fällen, in denen durch Lichtbildvergleiche eine Täterschaft ausgeschlossen wurde, konnte in neun Fällen trotzdem ein Beschuldigter ermittelt werden. Von den 19 Untersuchungseinheiten, die ganz ohne Identifizierungsurteil waren, wurden anderweitig 15 aufgeklärt. Auch in neun der 18 Fälle schwach negativ beurteilter Lichtbildvergleiche wurde auf andere Weise noch ein Beschuldigter ermittelt, siehe *Tabelle 10*.

Die Fälle schwach positiv beurteilter Lichtbildvergleiche müssen differenzierter betrachtet werden. Hier wurde in 7 Fällen der Tatverdächtige, bei dem der Lichtbildvergleich auf eine Täterschaft hindeutete als Beschuldigter geführt. In 2 Fällen hat sich durch Ermittlungen ein anderer Beschuldigter ergeben. In 3 Fällen, wo nicht ausgeschlossen werden konnte, dass es sich bei dem Tatverdächtigen und dem Täter um ein- und dieselbe Person handelt, wurde er trotzdem als Beschuldigter eingetragen. In 3 Fällen wurde letztlich ein anderer Beschuldigter eingetragen.

Identifizierung * Aufklärung Kreuztabelle

Anzahl

		Aufklärung		
		Nein	Ja	Gesamt
Identifizierung	Nichtidentifizierung	5	9	14
	Identifizierung	0	28	28
	schwach positiv	7	15	22
	schwach negativ	10	11	21
	ohne Angabe	4	15	19
Gesamt		26	78	104

Tabelle 10: Aufklärung der Straftaten in Verbindung mit der Identifizierung (LV)

Im Ergebnis trägt der Lichtbildvergleich nicht erheblich zur Aufklärung von Straftaten bei.

8.3 Zwischenfazit

Die computergestützte Gesichtserkennung beruht meistens auf Passbildern. Den Lichtbildvergleichen liegt zu fast 60 % Videoüberwachungsmaterial zugrunde. Allerdings ist bei beiden Ermittlungsmethoden festzustellen, dass die Qualität der Videobeweise in der Mehrzahl schlecht ist. Gesichtserkennungsverfahren tragen nicht erheblich zur Identifizierung bzw. Überführung von Tatverdächtigen bei. Im Falle der computergestützten Gesichtserkennung trugen Videobeweise im Jahr 2016 überhaupt nicht zur Identifizierung von Straftätern bei. Im Fall der Lichtbildvergleiche führten Videobeweise überwiegend nur zu schwachen Prädikaten. Bei Lichtbildvergleichen werden Täter außerdem überwiegend bei guter Bildqualität identifiziert, während bei der computergestützten Gesichtserkennung für die Identifizierung nicht nur die gute Qualität, sondern auch der Umfang der Referenzdatenbank eine entscheidende Rolle spielt.

Von den 166 Ermittlungsverfahren, die durch die beiden bildbasierten Ermittlungsmethoden der Gesichtserkennung nicht vorangebracht werden konnten, wurden 97 auf andere Art und Weise trotzdem aufgeklärt (58,4 %).

9 Untersuchungsergebnisse der Öffentlichkeitsfahndung

In Hessen gab es im Bezugszeitraum 2016 insgesamt 98 Ermittlungsöffentlichkeitsfahndungen. Es bleiben vier Fahndungen der Flächenpräsidien unberücksichtigt, da sie für andere Bundesländer oder die Bundespolizei in Hessen publiziert wurden und die originäre Zuständigkeit und Sachbearbeitung der Fälle sowie ggf. auch die Tatorte nicht in Hessen lagen. Der Auswertung liegen mithin 94 Identifizierungsöffentlichkeitsfahndungen zugrunde.

9.1 Ergebnisse der Öffentlichkeitsfahndung

Das PP Frankfurt hatte mit einer Anzahl von 20 die meisten Identifizierungsöffentlichkeitsfahndungen. Das PP Nordhessen hatte 18 Ermittlungsöffentlichkeitsfahndungen. Das Polizeipräsidium Mittelhessen hatte 15 und Westhessen 14 dieser Fahndungen. Das PP Südhessen sowie das PP Südosthessen hatten beide zwölf Ermittlungsöffentlichkeitsfahndungen. Die wenigsten Identifizierungsöffentlichkeitsfahndungen hatte das Polizeipräsidium Osthessen mit drei.

Abbildung 8: Verteilung der Ermittlungsöffentlichkeitsfahndung in Hessen

Forschungshypothese 1: *Ermittlungsöffentlichkeitsfahndungen beruhen öfter auf Bildern aus Videoüberwachungsanlagen als auf Bildern anderer Quellen*.
56 von 94 Ermittlungsöffentlichkeitsfahndungen beruhten auf Videoüberwachungsmaterial. Davon verteilen sich 49 Fahndungen auf Videoüberwachungsmaterial privater Institutionen, fünf auf staatliches Videoüberwachungsmaterial und zwei auf Videoüberwachungsmaterial aus Videoüberwachungsanlagen von Privatpersonen.
34 Fahndungen beruhten auf Phantombildern und vier auf Privataufnahmen.

Bildmaterial

		Häufigkeit	Prozent	Gültige Prozente	Kumulierte Prozente
Gültig	Phantombild	34	36,2	36,2	36,2
	Privataufnahme	4	4,3	4,3	40,4
	Videoüberwachung privat	49	52,1	52,1	92,6
	Videoüberwachung Privatperson	2	2,1	2,1	94,7
	Videoüberwachung staatlich	5	5,3	5,3	100,0
	Gesamt	94	100,0	100,0	

Tabelle 11: Aufschlüsselung des Bildmaterials (ÖF)

Die Forschungshypothese wurde bestätigt. Ermittlungsöffentlichkeitsfahndungen beruhten zu insgesamt 59,6 % auf Videoüberwachungsmaterial.

Forschungshypothese 2: *Die Bildqualität der Aufnahmen aus Videoüberwachungsanlagen ist überwiegend schlecht*.
39 der 49 Videobeweise aus Videoüberwachungsanlagen privater Institutionen hatten schlechte Qualität. Einer von zwei Videobeweisen aus Videoüberwachungsanlagen von Privatpersonen war schlecht. Alle fünf Videobeweise aus staatlicher Videoüberwachung waren zu schlecht, um eine zweifelsfreie Identifizierung zu gewährleisten. Insgesamt waren 45 der 56 Videobeweise schlechter Qualität.
Das Bildmaterial aus fotografischen Privataufnahmen war immer gut. Wie eingangs erwähnt, beruhen Phantombilder auf Personenbeschreibungen von Augenzeugen mit Wiedererkennungswert, weshalb diese von vornherein als gut eingestuft wurden.

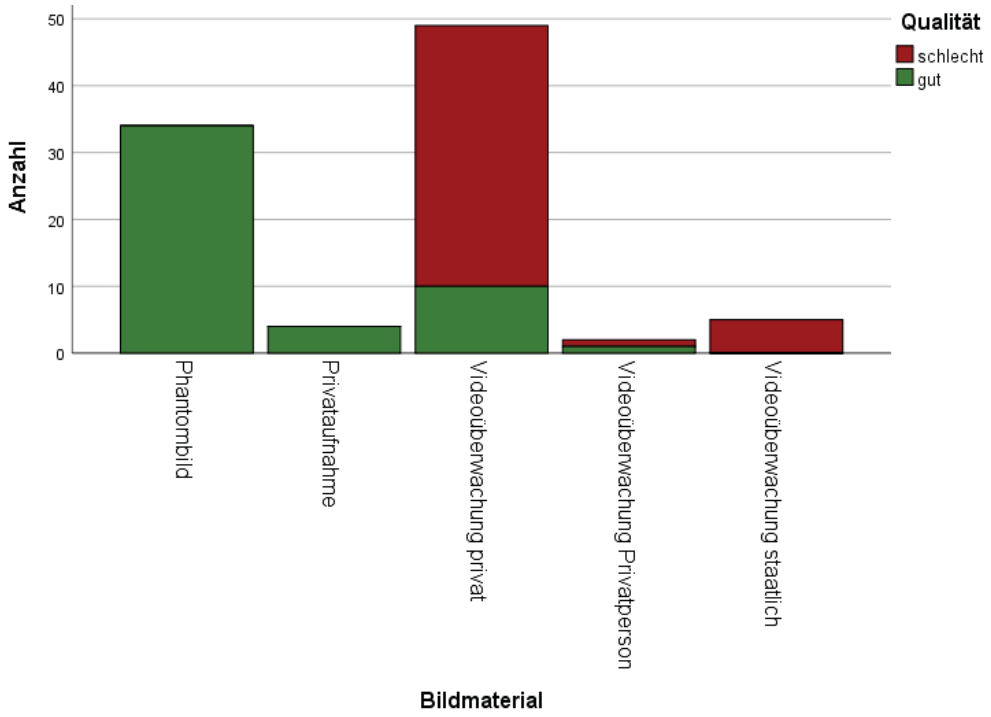

Abbildung 9: Qualitätsverteilung aller Bildquellen (ÖF)

Die Forschungshypothese wurde bestätigt. Die Bildqualität der Aufnahmen aus Videoüberwachungsanlagen ist überwiegend schlecht.

Forschungshypothese 3: Ermittlungs*öffentlichkeitsfahndung trägt erheblich zur Identifizierung von Straftätern bei*.

Bei 49 der 94 Straftaten wurde durch die Ermittlungsöffentlichkeitsfahndung bis zum Abgabetermin dieser Arbeit kein Tatverdächtiger identifiziert. Bei 45 der 94 Straftaten wurde ein Tatverdächtiger ermittelt. Es kann jedoch nicht gesagt werden, ob die Identifizierung aufgrund der Ermittlungsöffentlichkeitsfahndung erfolgte. Schon ohne dieses Wissen kann sicher gesagt werden, dass mindestens bei über der Hälfte der Straftaten (52,1 %) keine Identifizierung stattfand.

Identifizierung

		Häufigkeit	Prozent	Gültige Prozente	Kumulierte Prozente
Gültig	nein	49	52,1	52,1	52,1
	unbekannt	45	47,9	47,9	100,0
	Gesamt	94	100,0	100,0	

Tabelle 12: Häufigkeitsverteilung der Identifizierung eines Tatverdächtigen (ÖF)

Ermittlungsöffentlichkeitsfahndung trägt nicht erheblich zur Identifizierung von Tatverdächtigen bei. Die Forschungshypothese wurde widerlegt.

Forschungshypothese 4: *Videoüberwachung trägt dabei öfter zur Identifizierung von Straftätern bei als andere Bildquellen*.
In 27 der 56 Ermittlungsöffentlichkeitsfahndungen, die auf Videobeweisen beruhten, konnte durch die Maßnahme kein Tatverdächtiger identifiziert werden (48,2 %). In den anderen 29 Fahndungsfällen gibt es einen Tatverdächtigen, wobei unbekannt ist, ob dessen Identifizierung auf den Videobeweis zurückgeht. Bei den anderen Bildquellen konnte in 22 von 38 Ermittlungsöffentlichkeitsfahndungen kein Tatverdächtiger ermittelt werden (57,9 %). In 16 Fällen wurde ein Tatverdächtiger auf unbekannte Art und Weise ermittelt.
Bei den Videobeweisen liegt der Anteil der nicht identifizierten Personen somit bei ca. 50 % und bei den anderen Bildquellen bei ca. 58 %.

Bildmaterial * Identifizierung Kreuztabelle

Anzahl

		Identifizierung		
		nein	unbekannt	Gesamt
Bildmaterial	Phantombild	20	14	34
	Privataufnahme	2	2	4
	Videoüberwachung privat	26	23	49
	Videoüberwachung Privatperson	1	1	2
	Videoüberwachung staatlich	0	5	5
Gesamt		49	45	94

Tabelle 13: Aufschlüsselung Identifizierung/ Bildmaterial (ÖF)

Im Ergebnis kann keine sichere Aussage darüber getroffen werden, wie oft Videoüberwachung und die anderen Bildquellen zur Identifizierung führten. Es kann nur mit Sicherheit gesagt werden, wie oft die jeweiligen Fahndungsmaßnahmen erfolglos waren. Ermittlungsöffentlichkeitsfahndungen, die auf Videomaterial beruhen, haben zumindest einen geringeren prozentualen Wert von Nichtidentifizierungen.

Forschungshypothese 5: *Straftäter werden durch Ermittlungsöffentlichkeitsfahndung öfter bei guter Bildqualität identifiziert*.

Es gab 45 Ermittlungsöffentlichkeitsfahndungen, deren Bildmaterial schlechter Qualität und 49 Ermittlungsöffentlichkeitsfahndungen, deren Bildmaterial guter Qualität war. Bei 28 der 49 Fahndungsmaßnahmen mit guter Bildqualität konnte trotzdem kein Tatverdächtiger identifiziert werden. Bei den restlichen 21 der 49 Ermittlungsöffentlichkeitsfahndungen mit guter Bildqualität ist unbekannt, ob die Identifizierung des Täters auf die Fahndung zurückgeht und somit auch, ob ein Zusammenhang mit der Bildqualität besteht.

Von 45 Fahndungsmaßnahmen mit schlechter Bildqualität blieben 21 ungeklärt. In 24 Untersuchungseinheiten konnte trotzdem ein Tatverdächtiger ermittelt werden. Auch hier kann nicht gesagt werden, wie viele der Tatverdächtigen, trotz des schlechten Bildmaterials, durch die Ermittlungsöffentlichkeitsfahndung identifiziert werden konnten.

Identifizierung * Qualität Kreuztabelle

Anzahl

		Qualität		
		schlecht	gut	Gesamt
Identifizierung	nein	21	28	49
	unbekannt	24	21	45
Gesamt		45	49	94

Tabelle 14: Verhältnis der Bildqualität zur Täteridentifizierung (ÖF)

Die Forschungshypothese kann nicht verifiziert oder bestätigt werden. Fest steht nur, dass 57,1 % der Fahndungsmaßnahmen mit gutem Bildmaterial nicht zur Täteridentifizierung führten.

Forschungshypothese 6: *Ermittlungsöffentlichkeitsfahndung trägt erheblich zur Aufklärung von Straftaten bei*.

49 von 94 Straftaten, bei denen eine Ermittlungsöffentlichkeitsfahndung zum Einsatz kam, konnten nicht aufgeklärt werden (52,1 %). Bei den verbleibenden 45 aufgeklärten Untersuchungseinheiten, können keine Rückschlüsse darauf gezogen werden, ob die Tataufklärung der Ermittlungsöffentlichkeitsfahndung zugeschrieben werden kann.

Identifizierung * Aufklärung Kreuztabelle

Anzahl

		Aufklärung		
		nein	ja	Gesamt
Identifizierung	nein	49	0	49
	unbekannt	0	45	45
Gesamt		49	45	94

Tabelle 15: Aufklärung der Straftaten (ÖF)

Die Forschungshypothese wurde widerlegt. Ermittlungsöffentlichkeitsfahndung trägt nicht erheblich zur Aufklärung von Straftaten bei.

9.2 Zwischenfazit

Die meisten Ermittlungsöffentlichkeitsfahndungen beruhten auf Videoüberwachungsmaterial. Die Bildqualität des Videoüberwachungsmaterials war jedoch überwiegend schlecht.

Bei 49 der 94 Identifizierungsfahndungen konnte durch die Maßnahme kein Täter identifiziert werden. Bei den 45 Untersuchungseinheiten, bei denen ein TV eingetragen wurde, kann retrograd nicht gesagt werden, ob sich der Erfolg auf die Fahndungsmaßnahme zurückführen lässt. Dies lässt ebenso den Schluss zu, dass die Ermittlungsöffentlichkeitsfahndung in mindestens 49 der 94 Fälle nicht zur Aufklärung der Straftat führte.

Es kann keine valide Aussage darüber getroffen werden, ob Videoüberwachung im Zusammenhang mit der Ermittlungsöffentlichkeitsfahndung öfter zur Identifizierung von Tatverdächtigen führt als andere Bildmaterialien. Es kann nur mit Sicherheit gesagt werden, dass der Anteil der anderen Bildmaterialien prozentual gesehen bei den nicht identifizierten Personen höher ist.

Es kann ebenso keine valide Aussage darüber getroffen werden, ob die Bildqualität der Bildbasis einer Ermittlungsöffentlichkeitsfahndung Einfluss auf die Identifizierung des Tatverdächtigen hat.

10 Diskussion

10.1 Zusammenfassung der Ergebnisse

Zusammengefasst stellen sich die Ergebnisse der Untersuchung wie folgt dar. Der Auswertung lagen 101 Fall computergestützter Gesichtserkennung, 104 Lichtbildvergleiche und 94 Ermittlungsöffentlichkeitsfahndungen zugrunde.
Sowohl die Ermittlungsöffentlichkeitsfahndungen als auch die Lichtbildvergleiche beruhten in den meisten Untersuchungseinheiten auf Videoüberwachungsmaterial. Nur die computergestützte Gesichtserkennung basierte häufiger auf Passbildern.
Die Auswertung aller drei Ermittlungsmethoden hat ergeben, dass die Qualität der Videobeweise in der Mehrzahl schlecht war.
Beide Gesichtserkennungsverfahren und auch die Ermittlungsöffentlichkeitsfahndung trugen nicht erheblich zur Identifizierung von Tatverdächtigen und somit zur Aufklärung von Straftaten bei.
Der Anteil der Videoüberwachung an den Identifizierungen lag bei der computergestützten Gesichtserkennung bei null, bei den Lichtbildvergleichen lagen die positiven Identifizierungen bei 14,8 %. Bei den Ermittlungsöffentlichkeitsfahndungen gibt es keine valide Aussage darüber, wie oft ein Tatverdächtiger auf der Basis von Videoüberwachungsmaterial identifiziert werden konnte. Sicher ist nur, dass bei 48,2 % der Untersuchungseinheiten, die auf Videobeweisen beruhten, kein Tatverdächtiger wiedererkannt wurde.
Für die Lichtbildvergleiche konnte bestätigt werden, dass Täter öfter bei guter Bildqualität sicherer identifiziert werden konnten. Bei der computergestützten Gesichtserkennung spielt nicht nur die Qualität der Bildbasis eine Rolle, sondern auch der Umfang der Referenzdatenbank. Auf der Grundlage der Datenbasis der Ermittlungsöffentlichkeitsfahndungen, kann keine valide Aussage über einen Zusammenhang zwischen der Bildqualität und der Identifizierung eines Tatverdächtigen bei der Fahndungsmaßnahme getroffen werden.

10.2 Beantwortung der Forschungsleitfragen

Abschließend können die eingangs gestellten Forschungsleitfragen durch die Ergebnisse wie folgt beantwortet werden.

Wie viele Fälle gab es im Jahr 2016, bei denen die computergestützte Gesichtserkennung, ein Lichtbildvergleich oder eine Ermittlungsöffentlichkeitsfahndung zum Einsatz kamen?
Die Datenerhebung ergab, dass das HLKA in 256 Fällen um ein Gesichtserkennungsverfahren ersucht wurde. Die Verfahren teilen sich ohne untersuchungsrelevante Abzüge in 106 computergestützte Gesichtserkennungen und 150 Lichtbildvergleiche auf. Im Bezugsjahr gab es hessenweit außerdem 98 Ermittlungsöffentlichkeitsfahndungen.

Auf welchem Bildmaterial beruhten diese Ermittlungsmethoden?
Die computergestützte Gesichtserkennung basiert auf Bildern erkennungsdienstlicher Behandlung, auf Lichtbildern aus Geschwindigkeitsüberwachungsanlagen, Passbildern, Privataufnahmen und Videoüberwachungsmaterial aus Videoüberwachungsanlagen privater Institutionen und von Privatpersonen. Die Bildbasis der Lichtbildvergleiche ist identisch. Hinzu kommen noch Bilder aus staatlicher Videoüberwachung und polizeiliche Fotografien, die nicht im Zusammenhang mit erkennungsdienstlichen Behandlungen entstanden sind. Ermittlungsöffentlichkeitsfahndungen beruhten auf Phantombildern, Privataufnahmen oder Bildern aus Videoüberwachungsanlagen privater und staatlicher Institutionen sowie von Privatpersonen, siehe *Tabelle 1, 6 und 11*.

Wie war die Qualität des Bildmaterials?
Passbilder, polizeiliche Fotografien und Privataufnahmen sind bei allen Ermittlungsmethoden überwiegend bis ausschließlich guter Qualität. Fotografien haben häufig weniger Störfaktoren und in der Regel eine zeitgemäß hohe Bildauflösung. Die Bilder aus Geschwindigkeitsüberwachungsanlagen und Videoüberwachungsanlagen sind überwiegend bis ausschließlich schlechter Qualität, siehe *Abbildung 4, 6 und 9*. Der Anteil der Bilder mit schlechter Qualität

aus der Kategorie Passbild erklärt sich dadurch, dass vielen dieser Ermittlungsverfahren keine digitalen Originalbilder, sondern Kopien oder sogar gescannte Kopien zugrunde lagen.

Wurde durch die Ermittlungsmethode ein Tatverdächtiger identifiziert?
Durch die computergestützte Gesichtserkennung konnte in elf Fällen ein Tatverdächtiger identifiziert werden (10,1 %). Mithilfe des Lichtbildvergleiches wurden 28 Täter der Straftat überführt (26,9 %). Es kann keine Aussage darüber getroffen werden, wie oft eine Ermittlungsöffentlichkeitsfahndung zur Identifizierung eines Täters geführt hat, siehe *Tabelle 2, 8 und 12*. Somit lässt sich zumindest für die Gesichtserkennungsverfahren festhalten, dass durch die Ermittlungsmethoden zwar Tatverdächtige identifiziert werden können, dass dies aber nicht sehr oft vorkommt.

Wie oft lagen diesen Ermittlungserfolgen Videobeweise zugrunde?
Keine der elf Identifizierungen durch computergestützte Gesichtserkennung beruhte auf Videoüberwachungsmaterial. Neun der 28 Lichtbildvergleiche, die eine Täterschaft verifizierten, beruhten auf Videobeweisen. Für die Ermittlungsöffentlichkeitsfahndung kann keine Aussage getroffen werden, wie viele der identifizierten Tatverdächtigen aufgrund von Videoüberwachungsmaterial wiedererkannt werden konnten. Es lässt sich für die Gesichtserkennungsverfahren festhalten, dass Videobeweise seltener bis gar nicht zu den Ermittlungserfolgen beitragen, siehe *Tabelle 3 sowie Abbildung 7*.

Werden die Täter bei gutem Bildmaterial häufiger identifiziert als bei schlechtem?
Bei der computergestützten Gesichtserkennung lag neun der elf Identifizierungen Bildmaterial guter Qualität zugrunde. Allerdings wurde auch bei 41 Fällen mit gutem Bildmaterial kein Tatverdächtiger ermittelt. Für die computergestützte Gesichtserkennung ist nicht nur die Qualität des Bildmaterials wichtig, sondern auch die Größe der Referenzdatenbank. 19 der 28 Lichtbildvergleiche, bei denen eine Täterschaft durch die Gutachter bestätigt wurde, basierten auf qualitativ gutem Bildmaterial. Es gab insgesamt 49 Ermittlungsöffentlichkeitsfahndungen, deren Bildmaterial den Täter gut erkennbar zeigten. Davon

wurden 28 trotzdem nicht wiedererkannt. Dies kann auch an einem kleineren Verbreitungsgrad oder einer geringeren medialen Präsenz gelegen haben. Bei den verbleibenden 21 Fahndungen mit guter Bildbasis, in denen letztlich ein Täter identifiziert wurde, kann keine Aussage darüber getätigt werden, ob die Fahndung zur Identifizierung beigetragen hat. Zumindest für die Gesichtserkennungsverfahren zeichnet sich ab, dass eine gute Bildqualität von Vorteil ist, siehe *Tabelle 4 und 9*.

Können die Straftaten noch aufgeklärt werden, wenn durch die bildbasierten Ermittlungsmethoden kein Tatverdächtiger ermittelt werden konnte?
Von 90 verbleibenden Fällen, die nicht durch die computergestützte Gesichtserkennung aufgeklärt werden konnten, wurden 46 auf andere Art und Weise gelöst (51,1 %). Von 86 verbleibenden Fällen, die nicht durch einen Lichtbildvergleich geklärt werden konnten, wurden 51 auf andere Art und Weise gelöst (59,3 %), siehe *Tabelle 5 und 10*. Bezüglich der Ermittlungsöffentlichkeitsfahndungen können keine validen Aussagen getroffen werden. Es besteht somit zumindest bei den Gesichtserkennungsverfahren eine ca. 50 prozentige Chance, dass die Straftaten auch durch andere Ermittlungsmethoden geklärt werden können.

10.3 Bedeutung der Ergebnisse für Theorie und Praxis

Es ist aus Sicht der Theorie nicht verwunderlich, dass die computergestützte Gesichtserkennung die einzige der drei Ermittlungsmethoden ist, die am häufigsten auf Passbildern und nicht auf Videoüberwachungsmaterial beruht. Bilder aus Videoüberwachungsanlagen enthalten allein schon durch deren Anbringung perspektivische Verzerrungen. Hinzu kommt, dass es auf Videoüberwachungsmaterial durch die Bewegungsabläufe selten direkte Frontalaufnahmen des Täters bis max. 15 Grad Neigung gibt und andere Störfaktoren zum Beispiel durch schlechte Lichtverhältnisse nicht ausbleiben. Passbilder eignen sich sowohl von ihrer Ausrichtung als auch ihrer hohen Auflösung am besten für den Abgleich mit den Bildern der erkennungsdienstlichen Behandlung in der Referenzdatenbank.

Dass das Bildmaterial aus Videoüberwachungsanlagen bei der Ermittlungsöffentlichkeitsfahndung und den Lichtbildvergleichen ganz vorne liegt, zeigt wiederum den hohen Stellenwert, den die Videoüberwachung trotzdem bei der kriminalistischen Arbeit einnimmt. Von diesem Standpunkt der Wichtigkeit aus, ist es umso bedauerlicher, dass die Qualität der Bilder aus Videoüberwachungsanlagen häufig so schlecht ist, dass man den Täter darauf nicht zweifelsfrei identifizieren oder detailliert vergleichen kann. Dadurch wurde jede Täteridentifizierung eher zum Glücksfall als zur Regel, ganz gleich welche der drei Ermittlungsmethoden es betraf.

Für die Praxis heißt das, dass man einer Ausweitung von Videoüberwachungsanlagen aus kriminalistischer Sicht nicht ohne Vorbehalte zustimmen kann. Eine Ausweitung impliziert zwar mehr Bildbeweise, aber zwangsläufig keine besseren. Die Ergebnisse zeigen, dass die Chance auf eine Aufklärung der Straftat durch eine Quantifizierung der Videobeweise nicht immanent steigt. Zudem geht mit dem Anstieg der Videoüberwachung und dem Anstieg der Bildbeweise auch ein Anstieg der zu bearbeitenden Daten einher. Hier könnten Strafverfolgungsbehörden an personelle Grenzen stoßen.[268]

Eine Lösung wäre, Videoüberwachungsanlagen technisch auf einen angemessenen und zeitgemäßen Stand zu bringen und dies durch die DIN zukünftig vorzuschreiben. Das würde zum einen Grundrechte schonen und zum anderen das Bildmaterial, auf welches bislang zugegriffen werden kann, qualitativ verbessern. Die Thesis konnte aufzeigen, dass eine gute Qualität von Lichtbildern bei der Täteridentifizierung nützlich ist. Die Bedeutung der Bildqualität zeigt sich besonders bei den Lichtbildvergleichen. Je höher die Auflösung, desto deutlicher bilden sich Individualmerkmale ab und desto mehr Merkmale lassen sich zur Identifizierung sicher bestimmen. Nur bei guter Bildqualität ist der wichtige Detailvergleich möglich. Das Ergebnis sind dann Prädikate, die eine höhere Wahrscheinlichkeit ausdrücken.

Diese Lösung führt juristisch gesehen zu einem Problem. Aus der Auswertung der Daten geht hervor, dass das meiste Videoüberwachungsmaterial zur Aufklärung von Straftaten in Hessen von privaten Institutionen bezogen wurde. Das heißt, dass Videobeweise meistens aus dem Einzelhandel, von Tankstellen oder zum Beispiel Banken stammt. Diese Institutionen können sich gegen

[268] Vgl. *Kudlacek*, Akzeptanz von Videoüberwachung, 16f.

Straftaten wie Raub, Erpressung, Diebstahl oder Betrug versichern, so dass ihnen durch die Straftat kein finanzieller Schaden entsteht.[269] In dem Augenblick, in dem ein Tatverdächtiger ermittelt wird, könnte die entsprechende Institution gem. § 86 VVG entweder ihre zivilrechtlichen (Schadenersatz-)Ansprüche bei dem Beschuldigten bzw. Verurteilten selber geltend machen müssen, oder die Versicherung zahlt zwar, versucht aber den Verantwortlichen in Regress zu nehmen. Die Aussichten, so den gesamten Schaden unbürokratisch und zeitnah ersetzt zu bekommen, dürften schlecht sein. Zumal zivilrechtliche Ansprüche in der Regel erst nach Abschluss des Strafverfahrens geltend gemacht werden können.[270] Außerdem entstehen den Institutionen und Versicherungen hohe Verwaltungs- und Personalkosten, um die Ansprüche gerichtlich durchzusetzen. Das Interesse der Institutionen, ihre Videoüberwachungsanlagen für eine effektivere Strafverfolgung zu verbessern, dürfte ihrem eigenen wirtschaftlichen Interesse und Risikomanagement entgegenstehen.

Gegen eine Ausweitung spricht weiterhin, dass Strafverfolgungsbehörden erkennbar keine validen und korrekten Aussagen über die Effizienz von Videoüberwachungsmaterial bei allen bildbasierten Ermittlungsmethoden treffen können. Entsprechende Daten werden in Hessen für die Ermittlungsöffentlichkeitsfahndung überhaupt nicht zentral erhoben und bleiben auf der Ebene der Sachbearbeiter stecken. Dabei ist gerade die Ermittlungsöffentlichkeitsfahndung durch ihre Öffentlichkeitswirksamkeit von zentraler Bedeutung und wird oft, wie eingangs dargestellt, argumentativ für sicherheitspolitische Entscheidungen herangezogen.

Diese Untersuchung hat ergeben, dass mindestens über die Hälfte der Ermittlungsöffentlichkeitsfahndungen sicher nicht zur Identifizierung des Tatverdächtigen geführt haben. Bei den verbliebenen Fahndungen besteht auch noch die Möglichkeit, dass der Tatverdächtige auf andere Art und Weise als durch den Bildbeweis identifiziert wurde. Es liegt somit nicht fern, dass einzelne Erfolgsfälle bewusst medial instrumentalisiert werden, um bei der Bevölkerung ein verzerrtes Bild der Eignung von Fahndungsmaßnahmen und Videoüberwachungsmaterial zu erzeugen. Die Ergebnisse der Auswertung zeigen nämlich auch, dass die Videoüberwachung keine Wunderwaffe und kein

[269] Vgl. *Janke*, Kompendium Wirtschaftskriminalität, 194.
[270] Vgl. *Foerster*, Transfer der Ergebnisse von Strafverfahren in nachfolgende Zivilverfahren, 107. Das gilt nicht für das Adhäsionsverfahren, welches hier aber bewusst nicht thematisiert werden soll.

Allheilmittel in der Verbrechensbekämpfung ist, obwohl sie als solches dargestellt und getestet wird.[271]

Soll die Kriminalistik einen fundierten und empirischen Beitrag zu entscheidenden sicherheitspolitischen Debatten leisten, muss sie auswerten können, welche Effizienz ihre Maßnahmen haben und unter Umständen, worauf das beruht. Es ist gleichwohl ihre Chance als Wissenschaft gesehen und (an)erkannt zu werden.[272]

10.4 Schwächen der Untersuchung

Eine Schwäche der Untersuchung liegt darin begründet, dass sie sich auf drei bildbasierte Ermittlungsmethoden bezieht. Es bleiben dadurch zum Beispiel die Fälle unberücksichtigt, bei denen das Bildmaterial polizeiintern zur Identifizierung des Tatverdächtigen allen Mitarbeitern zur Verfügung gestellt wurde. Eine Vielzahl von Identifizierungen könnte bereits im Vorfeld einer Ermittlungsöffentlichkeitsfahndung durch Intranet-Fahndungen stattgefunden haben. Die Intranet-Fahndung wird zudem bei Straftaten eingesetzt, denen keine Straftat von besonderer Bedeutung zugrunde liegt und für die wegen ihres Bagatellcharakters gar keine Öffentlichkeitsfahndung in Betracht kommt. Die Untersuchung ist dahingehend also nicht umfassend.

Eine weitere Schwäche ist der Umfang der Daten. In drei Fällen der computergestützten Gesichtserkennung konnten keine Angaben zur Aufklärung der Straftat gemacht werden, da die Vorgänge mit einem Satzschutz belegt waren. Zudem gestaltete sich die retrograde Erfassung der hessenweiten Daten zu den Ermittlungsöffentlichkeitsfahndungen schwierig. Die Datenbasis ist dahingehend unvollständig, dass nicht erhoben werden durfte, ob die Straftat durch die Identifizierung des Tatverdächtigen aufgrund der Öffentlichkeitsfahndung aufgeklärt wurde. Dies wirkt sich auch auf die Forschungshypothesen und Forschungsleitfragen aus, inwiefern Videoüberwachungsmaterial und Bildqualität eine Identifizierung beeinflussen. An dieser Stelle konnte nur eine negative Abgrenzung erfolgen und gesagt werden, in wie vielen Fällen die Ermittlungsöffentlichkeitsfahndung, das Videoüberwachungsmaterial und die Bildqualität

[271] Vgl. *Schnabel*, Die polizeiliche Videoüberwachung öffentlicher Orte in Niedersachsen, 879.
[272] Zum Streit über die Wissenschaftlichkeit der Kriminalistik und ihr Potenzial vgl. *De Vries*, Ist die Kriminalistik eine Wissenschaft? 217.

definitiv nicht zur Identifizierung eines Tatverdächtigen beitrugen. Hier zeigt die Studie Verbesserungsbedarf.
Die Ergebnisse lassen keine repräsentativen Rückschlüsse auf die Qualität staatlicher Videoüberwachung zu, da im landespolizeilichen Zuständigkeitsbereich noch verhältnismäßig wenige öffentlich zugänglichen Räume videoüberwacht sind. Bahnhöfe und Flughäfen etc. fallen in den Zuständigkeitsbereich der Bundespolizei und waren daher nicht Bestandteil der Arbeit.
Aus der Untersuchung resultieren mithin Fragestellungen, die sich für weitere Studien anbieten und das Bild über den Beitrag der Videoüberwachung zur Kriminalistik ergänzen würden. Zum einen wäre interessant, ob sich die Ergebnisse für den polizeiinternen Bereich der Intranet- Fahndung bestätigen lassen. Es ist zu vermuten, dass es wegen der geringeren rechtlichen Anforderungen erheblich mehr Intranet- Fahndungen als Ermittlungsöffentlichkeitsfahndungen gab. Will man ein ganzheitliches Bild über die Effektivität bildbasierter Ermittlungsmethoden zeichnen, dann sollte der Intranet-Fahndung Rechnung getragen werden. Ebenso interessant wäre es, ob sich die Ergebnisse auch auf bundespolizeilicher Ebene und für staatliche Videoüberwachung als zutreffend erweisen. Zum anderen lässt diese Untersuchung präventive Ermittlungen außen vor, die ebenfalls zur Kriminalitätsbekämpfung beitragen und vervollständigend beforscht werden könnten.

11 Resümee

Am Ende bleibt für die thematisierten bildbasierten Ermittlungsmethoden, analog der Erkenntnis über Videoüberwachung, festzustellen, dass sie immer nur Hilfsmittel und Möglichkeiten sind, niemals aber mit an Sicherheit grenzender Wahrscheinlichkeit die Aufklärung der Straftat versprechen.[273] Nichtsdestotrotz haben diese Methoden bei guter Bildqualität das Potenzial Straftäter in einem rechtsstaatlichen Verfahren zweifelsfrei zu überführen. Somit würden sie auch den kriminalistischen Anspruch auf Wahrheitsforschung erfüllen.
Im Kontext der bildbasierten Ermittlungsmethoden zur Videoüberwachung ist das Fazit ernüchternd. Für die computergestützte Gesichtserkennung ist Videoüberwachung fast unbedeutend. Denn durch die Zweidimensionalität des

[273] Vgl. *Bornewasser/Schulz*, Systematische Videoüberwachung am Beispiel einer Maßnahme in Brandenburg, 75ff.

Abgleichmechanismus sowie der Anfälligkeit des Verfahrens gegenüber Vermummung, Maskierung, Bemalung und weiterer Störfaktoren ist die Ermittlungsmethode zu unflexibel, um entsprechendes Bildmaterial zu verarbeiten. Für einen Lichtbildvergleich sind die Bilder aus Videoüberwachungsanlagen schon besser geeignet. Leider erlaubt die Qualität der Bilder, durch Störfaktoren und geringe Auflösung, oft keinen Detailvergleich. Das Ergebnis sind schwache Prädikate, die das Ermittlungsverfahren nicht wesentlich voranbringen. Für die Ermittlungsöffentlichkeitsfahndung sind kaum Aussagen darüber zulässig, wie hilfreich sie im Zusammenhang mit Videoüberwachung bei der Aufklärung von Straftaten ist. Strafverfolgungsbehörden können diese Frage ad hoc nicht beantworten. Für die alltägliche Ermittlungsarbeit entsteht daher gar kein direkter Nutzen, bei einer Ausweitung von Videoüberwachungsanlagen, egal ob konventionell oder intelligent. Wenn der Einsatz von mehr Videoüberwachungsanlagen nur durch einen direkten Nutzen gerechtfertigt werden kann, so wie es *Kudlacek* vorschlägt, dann darf die Aufklärung von Straftaten nicht als ausschlaggebendes Argument angeführt werden.[274]

In Anbetracht der erarbeiteten Fakten ist die aktuelle Entscheidungstendenz im Spannungsverhältnis Sicherheit und Freiheit zugunsten der Sicherheit, durch Ausweitung der Videoüberwachung im öffentlichen Raum, folglich zumindest fragwürdig. Es werden mit Beschluss der Bundesregierung weitere Gesetzespakete zukünftig der Videoüberwachung den Weg ebnen.[275] Man wird bereits beim Tanken, beim Einkaufen, bei Bankgeschäften sogar beim Busfahren videografiert, alltäglich, nahezu überall. Private Videoüberwachungsanlagen gibt es viele. Eine Ausweitung der Videoüberwachung durch den Staat würde Privatheit und Freiheit zusätzlich belasten. Die Entwicklung spricht somit nicht für ein ausgewogenes Verhältnis von Freiheit und Sicherheit.[276]

Die Ergebnisse zeigen zudem deutlich, dass für einen rechtsstaatlichen und kriminalistischen Nutzen das aus Videoüberwachungsanlagen resultierende Bildmaterial qualitativ erst besser werden muss, bevor es seinem guten Ruf als Identifizierungsmittel gerecht werden kann. Es sollte das Motto Qualität vor

---

[274] Vgl. *Kudlacek*, Akzeptanz von Videoüberwachung, 149.
[275] Vgl. *Bundesregierung*, Bessere Videoüberwachung für mehr Sicherheit, https://www.bundesregierung.de/Content/DE/Artikel/2016/12/2016-12-21-bessere-videoueberwachung.html, (25.08.2017).
[276] Vgl. *Dollinger/ Schmidt-Semisch*, Sicherer Alltag? 8f.

Quantität gelten. Auch wenn die Angst vor Terrorismus, die Akzeptanz der Bevölkerung gegenüber dem Einsatz technischer Mittel zu dessen Bekämpfung erhöht[277], darf dabei aus Alternativlosigkeit nicht auf die Videoüberwachung gesetzt werden. Es hat sich gezeigt, dass diese im konventionellen Bereich nicht so gut ist wie gedacht, oder willentlich konstruiert.
Der Schlüssel zu erfolgreicher Strafverfolgung(svorsorge) ist in erster Linie bessere Videoüberwachung, nicht mehr, auch wenn diese Aussage dem allgemeinen Tenor der Politik und den Forderungen von Funktionären wichtiger Strafverfolgungsorgane widerspricht.

[277] Vgl. *Kudlacek*, Akzeptanz von Videoüberwachung, 148f.

„They who can give up essential liberty to obtain a little temporary safety, deserve neither liberty nor safety.“[278]

[278] *Franklin*, Remarks on the Propositions, 333f.

Quellenverzeichnis

AG Bonn: Beschluss vom 21.04.2016, Az. 51 Gs-410 UJs 203/16-722/16, Öffentlichkeitsfahndung – erhebliche Straftat, S. 248. In: Neue Zeitschrift für Strafrecht – Rechtsprechungs-Report (NStZ-RR), Jahrgang 21, Heft 8, 2016.

Alexy, Robert: Aussprache und Schlussworte (Diskussionsbeitrag), S. 121 – 123. In: Staatszwecke im Verfassungsstaat - nach 40 Jahren Grundgesetz. Die Bewältigung der wissenschaftlichen und technischen Entwicklungen durch das Verwaltungsrecht. Berichte und Diskussionen auf der Tagung der Vereinigung der Deutschen Staatsrechtslehrer in Hannover vom 4. bis 7. Oktober 1989. Veröffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer (VVDStRL), Heft 48. Berlin 1990.

Ammicht Quinn, Regina: Intelligente Videoüberwachung: eine Handreichung, https://publikationen.uni-tuebingen.de/xmlui/bitstream/handle/10900/67099/Band11_Vidoe%C3%BCberwachung_Handreichung.pdf?sequence=1, abgerufen am 06.10.2017.

Andexinger, Manfred: Das Spannungsfeld Freiheit versus Sicherheit – eine historisch-philosophische Reflexion, S. 111 – 124. In: Dimensionen der Sicherheitskultur. Hans-Jürgen Lange/ Michaela Wendekamm/ Christian Endreß (Hrsg.). 1. Auflage. Wiesbaden 2014.

Apelt, Maja/ Möllers, Norma: Wie intelligente Videoüberwachung erforschen? Ein Resümee aus zehn Jahren Forschung zur Videoüberwachung, S. 585 – 593. In: Zeitschrift für Außen- und Sicherheitspolitik (ZFAS). Jahrgang 4, Heft 4, 2011.

Apple: Technische Daten zum iPhone X. https://www.apple.com/de/iphone-x/specs/, abgerufen am 23.09.2017.

Averdiek-Gröner, Detlef/ Frings, Christoph: Standardmaßnahmen im Ermittlungsverfahren. 1. Auflage. Hilden 2014.

Bäcker, Matthias: Kriminalpräventionsrecht. Eine rechtsetzungsorientierte Studie zum Polizeirecht, zum Strafrecht und zum Strafverfahrensrecht. 1. Auflage. Tübingen 2015.

Bajmel, Bianca: Datenschutz in sozialen Netzwerken. Die Öffentlichkeitsfahndung im Rahmen der Nutzung des sozialen Netzwerkes Facebook. Zugleich Diss. Universität Tübingen. 1. Auflage. Hamburg 2017.

Becker von, Peter: Straftäter und Tatverdächtige in den Massenmedien: Die Frage der Rechtmäßigkeit identifizierender Kriminalberichte. 1. Auflage. Baden-Baden 1979.

Belina, Bernd/ Germes, Melina: Kriminalitätskartierung als Methode der kritischen Kriminologie. In: Kriminologisches Journal (KrimJ), 2015. https://halshs.archives-ouvertes.fr/halshs-01245026/document, abgerufen am 29.08.2017.

Belina, Bernd: „Kriminalität" und „Raum". Zur Kritik der Kriminalgeographie und zur Produktion des Raumes, S. 129 – 147. In: Kriminologisches Journal (KrimJ). Jahrgang 32, Heft 2, 2000.

Belina, Bernd: Raum, Überwachung, Kontrolle. Vom staatlichen Zugriff auf städtische Bevölkerung. 1. Auflage. Münster 2006.

Belina, Bernd: Sicherheit durch Technik? Zur Videoüberwachung öffentlicher Räume. S. 115 – 127. In: E-Government und Stadtentwicklung. Lena Hatzelhoffer/ Michael Lobeck/ Wolfgang Müller/ Claus-Christian Wiegandt (Hrsg.). 1. Auflage. Berlin 2010.

Benfer, Jost/ Bialon, Jörg: Rechtseingriffe von Polizei und Staatsanwaltschaft. Voraussetzungen und Grenzen. 4. Auflage. München 2010.

Beulke, Werner: Strafprozessrecht. 13. Auflage. Heidelberg 2016.

Blindenbacher, Wolfgang/ Müller, Dieter: Intelligente Videoüberwachung im öffentlichen Raum, S. 29 – 34. In: Polizei, Verkehr und Technik (pvt). Heft 3, 2015.

Bornewasser, Manfred / Schulz, Franziska: Systematische Videoüberwachung am Beispiel einer Maßnahme in Brandenburg, S. 75 – 93. In: Polizeiliche Videoüberwachung öffentlicher Räume. Hans-Jörg Bücking (Hrsg.). 1. Auflage. Berlin 2007.

Bretthauer, Sebastian: Intelligente Videoüberwachung. Eine datenschutzrechtliche Analyse unter Berücksichtigung technischer Schutzmaßnahmen. Zugleich Diss. Universität Frankfurt am Main. 1. Auflage. Frankfurt am Main 2017.

Bundesamt für Sicherheit in der Informationstechnik (BSI): https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/BioFace/BioFaceIIBericht.pdf;jsessionid=E4ED769895DCC5E9FB946B42AC815F59.1_cid369?__blob=publicationFile&v=3, abgerufen am 30.10.2017.

Bundesamt für Sicherheit in der Informationstechnik (BSI): https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/BioP/BioPI.pdf?__blob=publicationFile&v=1, abgerufen am 30.10.2017.

Bundesamt für Sicherheit in der Informationstechnik (BSI): https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Biometrie/Gesichtserkennung_pdf.pdf?__blob=publicationFile, abgerufen am 29.10.2017.

Bundeskriminalamt (BKA): http://www.cytrap.eu/files/EU-IST/2007/pdf/2007-07-FaceRecognitionField-Test-BKA-Germany.pdf, abgerufen am 29.10.2017.

Bundeskriminalamt (BKA): https://www.tib.eu/de/suchen/download/?tx_tibsearch_search%5Bdocid%5D=TIBKAT%3A860865568&tx_tibsearch_search%5Bsearchspace%5D=tn&cHash=5435684b2f85792d4a1ae7a69723f683#downloadmark, abgerufen am 30.10.2017.

Bundesministerium der Justiz (BMJ): Pressemitteilung, Sicherheitsgesetze auf dem Prüfstand, http://presseservice.pressrelations.de/standard/result_main.cfm?aktion=jour_pm&r=462713, abgerufen am 09.09.2017.

Bundesministerium des Innern (BMI): Sicherheitsbahnhof Berlin Südkreuz, https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2017/08/gesichtserkennungstechnik-bahnhof-suedkreuz.html, abgerufen am 30.10.2017.

Bundesministerium für Bildung und Forschung (BMBF): https://www.sifo.de/de/sira-sicherheit-im-oeffentlichen-raum-1868.html, abgerufen am 29.10.2017.

Bundesministerium für Bildung und Forschung (BMBF): MisPel: Multi-Biometriebasierte Forensische Personensuche in Lichtbild- und Videomassendaten, https://www.sifo.de/de/mispel-multi-biometriebasierte-forensische-personensuche-in-lichtbild-und-videomassendaten-2105.html, abgerufen am 30.10.2017.

Bundesministerium für Bildung und Forschung (BMBF): MuViT: Mustererkennung und Video Tracking: sozialpsychologische, soziologische, ethische und rechtswissenschaftliche Analysen, https://www.sifo.de/de/muvit-mustererkennung-und-video-tracking-sozialpsychologische-soziologische-ethische-und-1950.html, abgerufen am 30.10.2017.

Bundesministerium für Bildung und Forschung: https://www.sifo.de/de/ges-3d-multi-biometrische-gesichtserkennung-2103.html, abgerufen am 30.10.2017.

Bundesministerium für Bildung und Forschung: Mehr Sicherheit durch verbesserte Gesichtserkennung, https://www.bmbf.de/files/Projekt_des_Monats_Januar_2016.pdf, abgerufen am 30.10.2017.

Bundesregierung: Bessere Videoüberwachung für mehr Sicherheit, vom 05. Mai 2017. https://www.bundesregierung.de/Content/DE/Artikel/2016/12/2016-12-21-bessere-videoueberwachung.html, abgerufen am 25.08.2017.

Bundesverfassungsgericht (BVerfG): Beschluss vom 23.02.2007, Az. 1 BvR 2368/06, Videoüberwachung öffentlicher Plätze, S. 688 – 691. In: Neue Zeitschrift für Verwaltungsrecht (NVwZ), Jahrgang 26, Heft 6, 2007.

Bundesverwaltungsgericht (BVerwG): Urteil vom 25.01.2012, Az. 6 C 9/11, Offene Videoüberwachung der Reeperbahn, S. 757 – 763. In: Neue Zeitschrift für Verwaltungsrecht (NVwZ), Jahrgang 31, Heft 12, 2012.

Burhoff, Detlef: Handbuch für das strafrechtliche Ermittlungsverfahren. 7. Auflage. Bonn 2015.

BVerfG: Urteil vom 02.03.2010, Az. 1 BvR 256/08 u. a. Verfassungswidrige Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten, S. 833 – 856. In: Neue Juristische Wochenschrift (NJW), Jahrgang 63, Heft 12, 2010.

BVerfG: Urteil vom 15.12.1983, Az. 1 BvR 209/83. Verfassungsrechtliche Überprüfung des Volkszählungsgesetzes 1983, S. 419 – 428. In: Neue Juristische Wochenschrift (NJW), Jahrgang 37, Heft 8, 1984.

Clages, Horst/ Ackermann, Rolf: Der rote Faden. Grundsätze der Kriminalpraxis. 13. Auflage. Heidelberg 2017.

Cognitec: Benutzeroberfläche der Software FaceVACS-DBScan, http://www.cognitec.com/facevacs-dbscan.html, abgerufen am 07.10.2017.

Dalby, Jakob: Sicherheitsgesetzgebung unter dem Eindruck von Terror, S. 87 – 100. In: Rechtshandbuch Zivile Sicherheit. Christoph Gusy/ Dieter Kugelmann/ Thomas Würtenberger (Hrsg.). 1. Auflage. Heidelberg 2017.

De Vries, Hinrich: Einführung in die Kriminalistik für die Strafrechtspraxis. 1. Auflage. Stuttgart 2015.

De Vries, Hinrich: Ist die Kriminalistik eine Wissenschaft? S. 213 – 217. In: Kriminalistik, Heft 4, 2008.

Deutsche Forschungsgemeinschaft: Quantitative Umfrage zu Videoüberwachung, Sicherheitsgefühl und Raumwahrnehmung an drei Standorten in Hamburg, http://gepris.dfg.de/gepris/projekt/5405691, abgerufen am 29.10.2017.

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BFDI): Videoüberwachung, https://www.bfdi.bund.de/DE/Datenschutz/Themen/Technische_Anwendungen/TechnischeAnwendungenArtikel/Videoueberwachung.html, abgerufen am 10.09.2017.

Diekmann, Andreas: Empirische Sozialforschung. Grundlagen, Methoden, Anwendungen. 9. Auflage. Hamburg 2014.

Dollinger, Bernd/ Schmidt-Semisch: Sicherheit und Alltag: Einführende Zugänge, S. 1 – 26. In: Sicherer Alltag? Politiken und Mechanismen der Sicherheitskonstruktion im Alltag. Bernd Dollinger/ Henning Schmidt-Semisch (Hrsg.). 1. Auflage. Wiesbaden 2016.

Eifler, Stefanie/ Brandt, Daniela: Erfahrungen mit Videoüberwachung im Überblick, S. 95 – 118. In: Polizeiliche Videoüberwachung öffentlicher Räume. Hans-Jörg Bücking (Hrsg.). 1. Auflage. Berlin 2007.

Feltes, Thomas: Videoüberwachung. Es ist erst der Anfang… aber aller Anfang ist bekanntlich schwer. Ein futuristisch-zynisches Szenario oder eine Aufforderung zu mehr „possipullity“? S. 181 – 192. In: Bewährungshilfe, Jahrgang 48, Heft 2, 2001.

Fischer, Susanne/ Masala, Carlo: Die Politik der Inneren Sicherheit nach 9/11, S. 1 – 9. In: Susanne Fischer/ Carlo Masala (Hrsg.). Innere Sicherheit nach 9/11. Sicherheitsbedrohungen und (immer) neue Sicherheitsmaßnahmen? 1. Auflage. Wiesbaden 2016.

Flöther, Choni: Überwachtes Wohnen. Überwachungsmaßnahmen im Wohnumfeld am Beispiel Bremen/Osterholz-Tenever. 1. Auflage. Münster 2010.

Foerster, Max: Transfer der Ergebnisse von Strafverfahren in nachfolgende Zivilverfahren. 1. Auflage. Tübingen 2008.

Franklin, Benjamin: Remarks on the Propositions, S. 333 – 334. In: Memoirs of the life and writings of Benjamin Franklin. William Temple Franklin (Hrsg.). 1. Auflage. Philadelphia 1818.

Gabriel, Peter/ Huckenbeck, Wolfgang/ Kürpiers, Frank: Über die Fragwürdigkeit der Berechnung einer Identitätswahrscheinlichkeit in anthropologischen Gutachten, S. 346 – 349. In: Neue Zeitschrift für Verkehrsrecht (NZV). 27. Jahrgang, Heft 8, 2014.

Gercke, Björn/ Julius, Karl-Peter/ Temming, Dieter/ Zöller, Mark A.: Heidelberger Kommentar. Strafprozessordnung. 5. Auflage. Heidelberg 2012.

Geyer, Steven: Bringen mehr Kameras, mehr Sicherheit? Über den Ausbau von Videoüberwachung im öffentlichen Raum streiten Wissenschaftler und Politiker: Eindeutige Schlüsse könne beide Gruppen nicht ziehen. In: Frankfurter Rundschau am 05.01.2017. http://www.fr.de/politik/sicherheitspolitik-bringen-mehr-kameras-mehr-sicherheit-a-736538, abgerufen am 25.08.2017.

Göll, Wolfram: Viele Straftaten bleiben ungesühnt, vom 11.07.2016. https://www.bayernkurier.de/inland/15311-viele-straftaten-bleiben-ungesuehnt/, abgerufen am 15.12.2017.

Groh, Kathrin/ Rosch, Philipp: Videoüberwachung. Flächendeckend und am Flughafen. Ein deutsch-englischer Vergleich, S. 123 – 148. In: Susanne Fischer/ Carlo Masala (Hrsg.). Innere Sicherheit nach 9/11. Sicherheitsbedrohungen und (immer) neue Sicherheitsmaßnahmen? 1. Auflage. Wiesbaden 2016.

Gusy, Christoph: Die „Schwere" des Informationseingriffs, S. 395 – 413. In: Staat, Verwaltung und Rechtsschutz, Festschrift für Wolf-Rüdiger Schenke zum 70. Geburtstag. Peter Baumeister/ Wolfgang Roth/ Josef Ruthig (Hrsg.). Berlin 2011.

Häder, Michael: Empirische Sozialforschung. Eine Einführung. 3. Auflage. Wiesbaden 2015.

Hälterlein, Jens/ Möllers, Norma: Deutungskonflikte um automatisierte Videoüberwachung. Zur sozialen Konstruktion einer Technologie als Instrument zur Kriminalitätsbekämpfung, S. 163 – 180. In: Grenzenlose Sicherheit? Gesellschaftliche Dimensionen der Sicherheitsforschung. Peter Zoche/ Stefan Kaufmann/ Harald Arnold (Hrsg.). 1. Auflage. Berlin 2016.

Heckmann, Dirk: Sicherheitsarchitektur im bedrohten Rechtsstaat – Neue Polizeibefugnisse zwischen gestalterischer Freiheit und grundrechtlicher Statik, S. 9 – 28. In: Blaschke, Ulrich/ Förster, Achim/ Lumpp, Stephanie/ Schmidt, Judith (Hrsg.), Sicherheit statt Freiheit? Staatliche Handlungsspielräume in extremen Gefährdungslagen. 1. Auflage. Berlin 2005.

Heindl, Robert: System und Praxis der Daktyloskopie und der sonstigen technischen Methoden der Kriminalpolizei. 3. Auflage. Berlin 1927.

Held, Cornelius: Intelligente Videoüberwachung. Verfassungsrechtliche Vorgaben für den polizeilichen Einsatz. Zugleich Diss. Universität Würzburg. 1. Auflage. Berlin 2014.

Hempel, Leon/ Metelmann, Jörg: Bild – Raum – Kontrolle. Videoüberwachung als Zeichen gesellschaftlichen Wandels, S. 9 – 21. In: Bild – Raum – Kontrolle. Videoüberwachung als Zeichen gesellschaftlichen Wandels. Leon Hempel/ Jörg Metelmann (Hrsg.). 1. Auflage. Frankfurt am Main 2005.

Hempel, Leon/ Töpfer, Eric: CCTV in Europe. Final report. http://www.urbaneye.net/results/ue_wp15.pdf, abgerufen am 29.10.2017.

Hempel, Leon: Zur Evaluation von Videoüberwachung. Methoden, Standards und Beispiele aus der Bewertungspraxis, S. 117 – 145. In: Surveillance Studies. Perspektiven eines Forschungsfeldes. Nils Zurawski (Hrsg.) 1. Auflage. Budrich 2007.

Hengfoss, Clarissa/ Mull, Günther/ Püschel, Klaus/ Jopp- van Well, Eilin: Herausforderung bei der Gesichtserkennung, S. 699 – 703. In: Kriminalistik. Heft 12, 2015.

Hochschule Bonn-Rhein-Sieg: FeGeb - Fälschungserkennung für die Gesichtsbiometrie mit aktivem NIR-Kamerasystem, https://www.h-brs.de/de/fegeb, abgerufen am 30.10.2017.

Hoffmann, Claus: Das Intranet. Ein Medium der Mitarbeiterkommunikation. Zugleich Diss. Universität Hohenheim. 1. Auflage. Konstanz 2001.

Hompel, Michael ten/ Büchter, Hubert/ Franzke, Ullrich: Identifikationssysteme und Automatisierung. 1. Auflage. Heidelberg 2008.

Huckenbeck, Wolfgang/ Gabriel, Peter/ Kürpiers, Frank: Identifikation lebender Personen anhand von Lichtbildern des Gesichts, S. 5 – 11. In Der medizinische Sachverständige (MedSach). 111. Jahrgang, Heft 1, 2015.

Humer, Stephan G./ Lederer, Anna: Von der konventionellen zur intelligenten Videoüberwachung – Chancen und Risiken für Polizei und Gesellschaft, S. 36 – 39. In: Der Kriminalist. Jahrgang 48, Heft 10, 2016.

Janke, Günter: Kompendium Wirtschaftskriminalität. 1. Auflage. Frankfurt am Main 2008.

Joecks, Wolfgang: Studienkommentar StPO. 4. Auflage. München 2015.

Katz, Alfred: Staatsrecht. Grundkurs im öffentlichen Recht. 18. Auflage. Heidelberg 2010.

Klamt, Martin: Verortete Normen. Öffentliche Räume, Normen, Kontrolle und Verhalten. 1. Auflage. Wiesbaden 2007.

Klauser, Francisco R.: Die Videoüberwachung öffentlicher Räume. Zur Ambivalenz eines Instruments sozialer Kontrolle. 1. Auflage. Frankfurt 2006.

Kube, Edwin/ Störzer, Hans Udo/ Timm Klaus Jürgen: Kriminalistik. Handbuch für die Praxis und Wissenschaft. Band 2. 1. Auflage. Stuttgart 1994.

Kube, Edwin: Beweisverfahren und Kriminalistik in Deutschland. Ihre geschichtliche Entwicklung. In: Kriminologische Schriftenreihe der Deutschen Kriminologischen Gesellschaft, Dr. Armand Mergen (Hrsg.). Hamburg 1964.

Kubera, Thomas: Evaluation von Videoüberwachung in Bielefeld, S. 119 – 146. In: Polizeiliche Videoüberwachung öffentlicher Räume. Hans-Jörg Bücking (Hrsg.). 1. Auflage. Berlin 2007.

Kudlacek, Dominic: Akzeptanz von Videoüberwachung. Eine sozialwissenschaftliche Untersuchung technischer Sicherheitsmaßnahmen. Zugleich Diss. Universität Wuppertal. 1. Auflage. Wiesbaden 2015.

Kühling, Jürgen/ Seidel, Christian/ Sivridis, Anastasios: Datenschutzrecht. 1. Auflage. Frankfurt am Main 2008.

Lang, Holger: Staat, Macht, Eigentum und Freiheit: Eine politische Streitschrift. 1. Auflage. Norderstedt 2016.

Leopold, Nils: Rechtskulturbruch. Die Ausbreitung der Videoüberwachung und die unzulängliche Reaktion des Rechts, S. 273 – 292. In: Bild – Raum – Kontrolle. Videoüberwachung als Zeichen gesellschaftlichen Wandels. Leon Hempel/ Jörg Metelmann (Hrsg.). 1. Auflage. Frankfurt am Main 2005.

Mai, Dominik: Interaktive Karte. So gefährlich ist es auf Berlins U-Bahnhöfen, vom 13.03.2017. http://www.berliner-zeitung.de/berlin/verkehr/interaktive-karte-so-gefaehrlich-ist-es-auf-berlins-u-bahnhoefen-26177452,, abgerufen am 25.08.2017.

Marx, Gary T.: What's New About The New Surveillance? Classifying for Change and Continuity, S. 9 – 29. In: Surveillance & Society. Jahrgang 1, Heft 1, 2002.

McCahill, Michael: Beyond Foucault: towards a contemporary theory of surveillance, S. 41 – 65. In: Surveillance, Closed Circuit Television and Social Control. Clive Norris/ Jade Moran/ Gary Armstrong (Hrsg.). 1. Auflage. Aldershot 1998.

Medjedovic, Irena: Qualitative Sekundäranalyse. Zum Potenzial einer neuen Forschungsstrategie in der empirischen Sozialforschung. Zugleich Diss. phil. Uni Bremen. 1. Auflage. Wiesbaden 2014.

Meier, Stefanie/ Lütolf, Daniel/ Schillerwein, Stephan: Herausforderung Intranet. Zwischen Informationsvermittlung, Diskussionskultur und Wissensmanagement. 1. Auflage. Wiesbaden 2014.

Mergen, Armand: Die Wissenschaft vom Verbrechen. Eine Einführung in die Kriminologie. 1. Auflage. Hamburg 1961.

Metag, Katharina/ Bruns, Hildburg: Zwei Straftaten aufgeklärt. Soso, lieber Senat, Kamera-Überwachung bringt also nichts, vom 29. Dezember 2016. http://www.bz-berlin.de/berlin/friedrichshain-kreuzberg/soso-lieber-senat-kamera-ueberwachung-bringt-also-nichts, abgerufen am 26.08.2017.

National Institute for Standardization: Face Projects, https://www.nist.gov/programs-projects/face-projects, abgerufen am 30.10.2017.

Nouak, Alexander: Grenzen der Gesichtserkennung. So kann Videoüberwachung überlistet werden, S. 14 – 16. In: Zeitschrift für die Sicherheit der Wirtschaft (WIK). Heft 4, 2013.

O. V.: Intelligent information system supporting observation, searching and detection for security of citizens in urban environment, http://www.indect-project.eu/, abgerufen am 29.10.2017.

O. V.: Summary of the 3D Face Project, https://www.3dface.org/project.html, abgerufen am 30.10.2017.

O.V.: Das Wortauskunftssystem zur deutschen Sprache in Geschichte und Gegenwart (DWDS), https://www.dwds.de/wb/fahnden, abgerufen am 21.10.2017.

Ogorek, Markus: Fortgeschrittenenhausarbeit – Öffentliches Recht: Polizeirecht – Im Auge des Betrachters, S. 811 – 816. In: Juristische Schulung (JuS) Jahrgang 53, Heft 9, 2013.

Pieroth, Bodo/ Schlink, Bernhard/ Kniesel, Michael: Polizei- und Ordnungsrecht mit Versammlungsrecht. 9. Auflage. München 2016.

Polizei Hessen: Die Behörden und Einrichtungen der Polizei Hessen, https://www.polizei.hessen.de/Dienststellen/, abgerufen am 04.11.2017.

Polizeiliche Kriminalstatistik (PKS): Richtlinien für die Führung der Polizeilichen Kriminalstatistik in der Fassung vom 01.01.2017, https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/PolizeilicheKriminalstatistik/2016/pks2016Richtlinien.html, abgerufen am 11.11.2017.

Pretzel, Andrew: Warum die Gesichtserkennung als Fahndungshilfe vorerst nicht einsatzfähig ist. Erkenntnisse aus dem Projekt „Foto-Fahndung“ am Mainzer Hauptbahnhof, S. 42 – 44. In: POLIZEI-heute. Heft 2, 2008.

Ranftl, Andreas G.: Digitale Gesichtserkennung. Theoretischer Überblick und praktische C++-Implementierung. 1. Auflage. Hamburg 2012.

Rolfes, Manfred: Kriminalität, Sicherheit und Raum. Humangeographische Perspektiven der Sicherheits- und Kriminalitätsforschung. 1. Auflage. Stuttgart 2015.

Rommert, Frank-Michael: Hoffnungsträger Intranet. Charakteristika und Aufgaben eines neuen Mediums in der internen Kommunikation. 1. Auflage. München 2002.

Schenke, Wolf-Rüdiger: Polizei- und Ordnungsrecht. 9. Auflage. Heidelberg 2015.

Schnabel, Christoph: Die polizeiliche Videoüberwachung öffentlicher Orte in Niedersachsen, S. 879 – 881. In: Datenschutz und Datensicherheit (DuD), Heft 12. Wiesbaden 2011.

Schneider, Heiko: Polizeiliche Fahndung – neue Wege zum Erfolg, S. 24 – 27. In: Deutsche Polizei, Jahrgang 52, Heft 1, 2003.

Scholze-Stubenrecht, Wolfgang: Duden. Deutsches Universal Wörterbuch. Das umfassende Bedeutungswörterbuch der deutschen Gegenwartssprache. 8. Auflage. Berlin 2015.

Schroer, Markus: Sehen, Beobachten, Überwachen. Beitrag zu einer Soziologie der Aufmerksamkeit, S. 325 – 341. In: Bild – Raum – Kontrolle. Videoüberwachung als Zeichen gesellschaftlichen Wandels. Leon Hempel/ Jörg Metelmann (Hrsg.). 1. Auflage. Frankfurt am Main 2005.

Shakespeare, William: König Lear. 3. Auflage. Berlin 2015.

Sigmund, Thomas: Allein unter Feinden? Was der Staat für unsere Sicherheit tut – und was nicht. 1. Auflage. Freiburg 2017.

Soiné, Michael: Ermittlungsverfahren und Polizeipraxis. Einführung in das Strafverfahrensrecht. 1. Auflage. Heidelberg 2013.

Stettner, Elisa: Sicherheit am Bahnhof. Überwachungsmaßnahmen zur Abwehr terroristischer Anschläge. 1. Auflage. Berlin 2017.

Störzer, Hans Udo: Zur Geschichte der Fahndung. Einführende Betrachtung. S. VII – XXXII. In: Bibliografie Fahndung. Hefele, Bernhard (Hrsg.). 1. Auflage. Wiesbaden 1979.

Ströbel, Lukas: Persönlichkeitsschutz von Straftätern im Internet. Zugleich Diss. jur. Passau. 1. Auflage. Baden-Baden 2016.

Thiel, Wolfgang: Identifizierung von Personen. 1. Auflage. Hilden 2006.

Tomii, Yasushi/ Scheer, Steffen: Gesichtserkennung, https://www2.informatik.hu-berlin.de/Forschung_Lehre/algorithmenII/Lehre/SS2004/Biometrie/05Gesicht/gesichtserkennung.pdf#page=4&zoom=auto,-82,656, abgerufen am 07.10.2017.

Töpfer, Eric: Die Kamera als Waffe? Videoüberwachung und der Wandel des Krieges. S. 257 – 272. In: Bild – Raum – Kontrolle. Videoüberwachung als Zeichen gesellschaftlichen Wandels. Leon Hempel/ Jörg Metelmann (Hrsg.). 1. Auflage. Frankfurt am Main 2005.

VG Halle: Videoüberwachung eines öffentlichen Platzes, S. 164. In: Landes- und Kommunalverwaltung (LKV), 10. Jahrgang, Heft 4, 2000.

VG Karlsruhe: Videoüberwachung öffentlicher Räume, S. 117 – 118. In: Neue Zeitschrift für Verwaltungsrecht (NVwZ), 21. Jahrgang, Heft 1, 2002.

Walder, Hans/ Hansjakob, Thomas: Kriminalistisches Denken. 10. Auflage. Heidelberg 2016.

Weichert, Thilo: Praxis und rechtliche Aspekte optischer Überwachungsmethoden – zum Einsatz moderner Videotechnik, S. 4-57. In: Datenschutz-Nachrichten (DANA), Sonderheft Videoüberwachung. Deutsche Vereinigung für Datenschutz DVD e. V. (Hrsg.). Bonn 1988.

Weichert, Thilo: Private Videoüberwachung und Datenschutzrecht. https://www.datenschutzzentrum.de/video/videpriv.htm, abgerufen am 17.09.2017.

Wirth, Ingo: Kriminalistik-Lexikon. 4. Auflage. Heidelberg 2011.

Zurawski, Nils/ Czerwinski, Stefan: ‚Sie sind doch auch für Videoüberwachung, oder…?' Warum Umfragen zu Kameraüberwachung nicht unbedingt eine Antwort auf das geben, was sie eigentlich wissen wollen, S. 214 – 220. In: Der Kriminalist. Jahrgang 39, Heft 5, 2007.

Zurawski, *Nils*: Surveillance Studies, http://www.surveillance-studies.org/forschernetzwerk/forschungsstandorte-surveillance-studies/, abgerufen am 29.10.2017.

Zurawski, Nils: Videoüberwachung. Praktische Überlegungen zu einer allgegenwärtigen Technologie, S. 396 – 410. In: Medien – Macht – Demokratie. Neue Perspektiven. Lothar Bisky/ Konstanze Kriese/ Jürgen Scheele (Hrsg.). 1. Auflage. Berlin 2009.

Anhang

Die verwendeten und erhobenen Datensätze werden aus datenschutzrechtlichen Gründen an dieser Stelle nicht veröffentlicht.

Erklärung

„Hiermit erkläre ich, dass ich die vorliegende Masterthesis selbstständig verfasst und keine anderen als die angegebenen Hilfsmittel benutzt habe. Die Stellen der Thesis, die anderen Quellen im Wortlaut oder dem Sinn nach entnommen wurden, sind durch Angaben der Herkunft kenntlich gemacht. Personen in Abbildungen waren mit ihrer Darstellung ausdrücklich einverstanden. Die Arbeit wurde nicht anderweitig als Prüfungsleistung verwendet."

Taunusstein, den 29.01.2018

(Im Original unterschrieben)

Anika Kepert