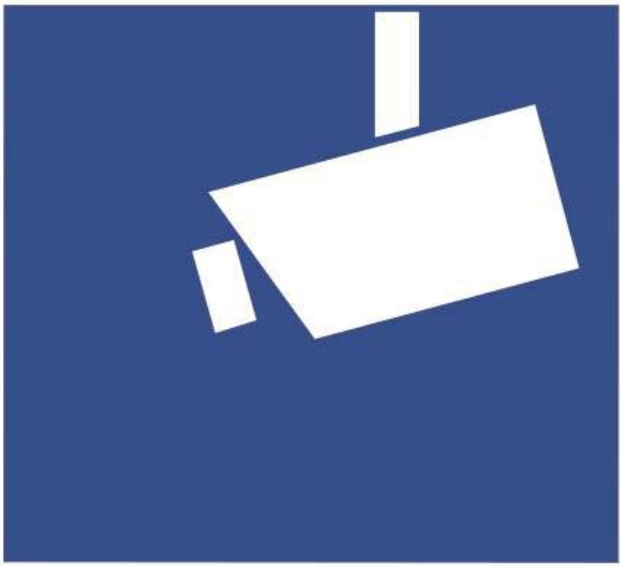
Ruhr-Universität Bochum
Juristische Fakultät - Lehrstuhl für Kriminologie
Masterstudiengang Kriminologie, Kriminalistik und Polizeiwissenschaft

Masterthesis

„Für Ihre Sicherheit wird dieser Bereich videoüberwacht“



Der polizeiliche Einsatz von Videoüberwachung öffentlich zugänglicher Räume unter Berücksichtigung „intelligenter“ Systeme

vorgelegt von

Christoph Sehrt

Februar 2018

Erstgutachter: Dr. Andreas Ruch

Zweitgutachter: M.Sc. Roger Jäger

Inhaltsverzeichnis

Abkürzungen

Abbildungen

Abkürzungen

Abb.	Abbildungen
Abs.	Absatz
AG	Amtsgericht
Art.	Artikel
ASIP	application-specific information processing
APFeI	Analyse von Personenbewegungen an Flughäfen mittels zeitlich rückwärts- und vorwärtsgerichteter Videodatenströme
Az	Aktenzeichen
BayPAG	Gesetz über die Aufgaben und Befugnisse der Bayerischen Staatlichen Polizei
BayRS	Bayerische Rechtssammlung
BbgPolG	Brandenburgisches Polizeigesetz
BGBl	Bundesgesetzblatt
BGH	Bundesgerichtshof
BDSG	Bundesdatenschutzgesetz
BKA	Bundeskriminalamt
BMBF	Bundesministerium für Bildung und Forschung
BMI	Bundesministerium des Innern
BMVIT	Bundesministerium für Verkehr, Innovation und Technologie
BOA	Behavioral Observation Analysis
BPA	Bundespersonalausweis
BPolG	Bundespolizeigesetz
bspw.	beispielsweise
BT	Bundestag

BVerfG	Bundesverfassungsgericht
BVerwG	Bundesverwaltungsgericht
CCTV	Closed circuit television (Videoüberwachung)
CDU	Christlich Demokratische Union Deutschlands
DB AG	Deutsche Bahn Aktiengesellschaft
G20	Gruppe der 20 (wichtigsten Industrie- und Schwellenländer)
gem.	gemäß
GES-3D	Multi-Biometrische Gesichtserkennung – Dreidimensional
GG	Grundgesetz
GPS	Global Positioning System
GVBl	Gesetz- und Verordnungsblatt
HLKA	Hessisches Landeskriminalamt
HmbGVBl	Hamburgisches Gesetz- und Verordnungsblatt
HmbPolDVG	Gesetz über die Datenverarbeitung der Polizei Hamburg
Hrsg.	Herausgeber
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung
IDF	Identitätsfeststellung
INPOL	Informationssystem Polizei
IMU	inertial measurement unit
iVÜ	intelligente Videoüberwachung
Kfz	Kraftfahrzeug
KIT	Karlsruher Institut für Technologie
MisPel	Multi-Biometriebasierte Forensische Personensuche in Lichtbild- und Videomassendaten

MisPel-S	Multi-Biometriebasierte Forensische Personensuche in Lichtbild- und Videomassendaten - Teilvorhaben: sozialwissenschaftliche Begleitforschung
Muskat	Multisensoriell gestützte Erfassung von Straftätern in Menschenmengen bei komplexen Einsatzlagen
MuViT	Mustererkennung und Video Tracking: sozialpsychologische, soziologische, ethische und rechtswissenschaftliche Analysen
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NZG	Nicht zuzuordnender Gegenstand
ÖPNV	Öffentlicher Personennahverkehr
OVG	Oberverwaltungsgericht
PAuswG	Personalausweisgesetz
PC	Personal Computer
PDV	Polizeidienstvorschrift
PolG NRW	Polizeigesetz des Landes Nordrhein-Westfalen
Rn.	Randnummer
Soko	Sonderkommission
StPO	Strafprozessordnung
u.a.	und andere
USBV	Unkonventionelle Spreng- oder Brandvorrichtung
VÜ	Videoüberwachung
Sifo	Sicherheitsforschung
ZD	Zeitschrift für Datenschutz

Abbildungen

A Einleitung

Videoüberwachung ist heutzutage allgegenwärtig. Die Bevölkerung hat sich seit ihrer Einführung vor fast 60 Jahren[1] längst an Videokameras im öffentlichen Raum gewöhnt.[2] Es ist kaum mehr möglich, sich der Videoüberwachung zu entziehen. An Straßen, Plätzen, öffentlichen Gebäuden, im öffentlichen Personennahverkehr oder zu besonderen Anlässen, wie bei Fußballspielen und Weihnachtsmärkten, findet Videoüberwachung statt. Im nichtöffentlichen Bereich ist sie noch um ein Vielfaches höher.[3] Tankstelle, Supermärkte, Kaufhäuser und Hauseingänge sind mittlerweile mit Videotechnik ausgestattet. Genaue Zahlen gibt es nicht, da es zu viele verschiedene Bedarfsträger gibt und nach der Rechtslage in Deutschland keine Registrierung vorgesehen ist.[4]

Die Tendenz zum weiteren Ausbau der VÜ lässt sich darauf zurückführen, dass auf der einen Seite die Technik bei steigender Leistung und Qualität der Bildaufnahmen immer günstiger wird und dass auf der anderen Seite, der Ruf der Bürger[5] nach erhöhtem Schutz durch den offenen Videogeräteeinsatz immer lauter wird.[6] In Umfragen befürwortet regelmäßig die Mehrheit der Befragten den verstärkten Einsatz von Videoüberwachung. Je nach Umfrage schwanken die Zahlen zwischen 60 - 80%.[7] Auch wenn diese nicht immer repräsentativ sind, spiegeln sie doch eine Tendenz sowie eine Erwartungshaltung der Bevölkerung an diese Technik wider. Insbesondere nach Gewaltdelikten auf öffentlichen Plätzen und im Bereich des ÖPNV, aber auch bei (versuchten) Terroranschlägen steigt der Zuspruch signifikant.[8]

---

[1] Vgl. Held: Intelligente Videoüberwachung, S. 15.
[2] Vgl. Knape: Videogeräteeinsatz, S. 207.
[3] Vgl. Bergmann/Möhrle/Herb: BDSG, § 6b, Rn. 2.
[4] Vgl. BT-Drucksache 17/2750, S. 8f.
[5] Um den Textfluss zu gewährleisten wird in der vorliegenden Arbeit auf die Nutzung der weiblichen Anredeform weitestgehend verzichtet. Die Gültigkeit männlicher Anredeformen wird für beide Geschlechter unterstellt.
[6] Vgl. Knape: Videogeräteeinsatz, S. 207.
[7] Vgl. Umfrage des Meinungsforschungsinstituts YouGov für die Deutsche Presse-Agentur in Hamburger Abendblatt: Umfrage: Mehrheit der Deutschen für mehr Videoüberwachung vom 25.12.2016 auf https://www.abendblatt.de/politik/deutschland/article209084663/Umfrage-Mehrheit-der-Deutschen-fuer-mehr-Videoueberwachung.html, abgerufen am 11.11.2017; siehe auch Forsa-Umfrage in der Tagesspiegel: Berliner befürworten Ausbau der Videoüberwachung vom 30.01.2017 auf http://www.tagesspiegel.de/berlin/forsa-umfrage-berliner-befuerworten-ausbau-der-videoueberwachung/19324248.html, abgerufen am 11.11.2017.
[8] Schulz: Videoüberwachung: Mehr Kameras = Mehr Sicherheit?, S. 3.

In jüngster Vergangenheit ist die VÜ mehrfach in den medialen Fokus geraten. Mit dem sogenannten Videoüberwachungsverbesserungsgesetz beschloss der Gesetzgeber Anfang des Jahres 2017 ein Maßnahmenpaket zur „Erhöhung der Sicherheit in öffentlich zugänglichen großflächigen Anlagen und im öffentlichen Personenverkehr durch optisch-elektronische Einrichtungen“.[9] Zudem positionierten sich im Wahlkampf zu den Landtagswahlen 2017 in den jeweiligen Bundesländern und zur Wahl des deutschen Bundestages die Parteien zum Thema Videoüberwachung des öffentlichen Raumes deutlich. Da diese von vielen als Baustein der inneren Sicherheit verstanden wird, offenbarte sich der „traditionellen Rechts-Links-Dichotomie des politischen Spektrums“[10] folgend, eine große Bandbreite an Positionen - von einer unabdingbaren Notwendigkeit über verhaltene/gemäßigte Nutzung bis hin zur einer offenen Ablehnung der VÜ.[11] Am meisten in den medialen Fokus dürfte aber das gemeinsame Pilotprojekt des Bundesministeriums des Innern, der Bundespolizei, des Bundeskriminalamt und der Deutschen Bahn AG, „Sicherheitsbahnhof Berlin Südkreuz“, gerückt sein. Im Rahmen dieses Projektes soll mit freiwilligen Testpersonen im Echtzeitbetrieb die Wirksamkeit der sogenannten „Intelligenten Videoüberwachung“ getestet werden. Neben der Anwendung eines Gesichtserkennungssystems sollen verschiedene Gefahrenszenarien, wie hilflos, am Boden liegende Personen oder verdächtige Gegenstände automatisiert durch die Systeme erkannt und gemeldet werden.[12]

Der Versuch, intelligente Videoanalysen polizeilich nutzbar zu machen, ist nicht neu. Bereits seit dem Jahr 2000 testet das BKA die biometrische Gesichtserkennung. 2006 fand im Hauptbahnhof Mainz erstmals ein Test unter realen Bedingungen statt. Auch wenn die Trefferquote von rund 40 Prozent im Jahr 2002 auf knapp über 60 Prozent im Jahr 2006 gestiegen war, wurde der

---

[9] BGBl I 2017 Nr. 23, S. 968 ff.
[10] Frevel/Rinke: Innere Sicherheit als Thema parteipolitischer Auseinandersetzung, S. 8.
[11] Bspw. CDU: Für ein Deutschland, in dem wir gut und gerne leben. - Regierungsprogramm 2017 – 2021, S. 61 oder Wahlprogramm der Partei DIE LINKE zur Bundestagswahl 2017, S. 113 und BÜNDNIS 90/DIE GRÜNEN: Zukunft wird aus Mut gemacht - Bundestagswahlprogramm 2017, S. 136; siehe auch https://www.datenschutzbeauftragter-info.de/positionen-der-parteien-zum-thema-videoueberwachung/, abgerufen am 23.11.2017.
[12] Bundesministerium des Inneren: Sicherheitsbahnhof Berlin Südkreuz, Pressemitteilung vom 01.08.2017, auf https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2017/08/gesichtserkennungstechnik-bahnhof-suedkreuz.html, abgerufen am 23.11.2017.

Feldversuch seitens des BKA als nicht erfolgreich gewertet, da die Trefferquote bei ungünstigen Lichtverhältnissen, wie in der Dämmerung oder bei Nacht, auf 10 bis 20 Prozent sank.[13]

Seit diesem Pilotprojekt sind nunmehr zehn Jahre vergangen, während die technische Entwicklung unaufhaltsam fortgeschritten ist. Im zivilen Sektor hat sich die intelligente Videoanalyse zur Steigerung der Sicherheit und der Gefahrenreduzierung seither bereits etabliert. Moderne Fahrzeuge verfügen beispielsweise über eine Verkehrszeichenerkennung (Traffic Sign Detection)[14] und einen Müdigkeitswarner.[15] Apple Nutzer können ihre Daten schützen, indem sie das iPhone X mittels Face ID sperren und eine Authentifizierung via Gesichtserkennung erlauben.[16] Aber auch die Bundesregierung förderte seit dem Start des Sicherheitsforschungsprogramms im Jahr 2007 unterschiedlichste Forschungsprojekte im Bereich der zivilen Sicherheit, die sich mit „innovativen Verfahren zur automatischen Erfassung, gezielter Erkennung und Verarbeitung von Daten aus unterschiedlichen Quellen, wie beispielsweise Kameras und Sensoren“[17] befassen. Hierunter fielen auch Projekte, die ihre Forschung gezielt auf die Wirksamkeit und den Mehrwert intelligenter Videoüberwachung und -analyse für die Strafverfolgungsbehörden ausrichteten.[18]

Einige dieser Projekte waren zumindest aus Sicht der Forscher und Auftraggeber erfolgreich und werden deshalb im Folgenden eingehender betrachtet. Vorab werden einige begriffliche und technische Grundlagen erläutert, um ein besseres Verständnis der Thematik zu vermitteln. Weiterhin wird der Perspektive der intelligenten VÜ nachgegangen und ihr Mehrwert gegenüber der konventionellen VÜ beleuchtet.

---

[13] Vgl. Held: Intelligente Videoüberwachung, S. 25.
[14] Produktbeschreibung Hella Aglaia auf http://www.aglaia-gmbh.de/verkehrszeichenerkennung, abgerufen am 24.11.2017.
[15] Karrer-Gauß: Prospektive Bewertung von Systemen zur Müdigkeitserkennung, S. 65.
[16] Apple: Informationen zur fortschrittlichen Technologie von Face ID auf https://support.apple.com/de-de/HT208108, abgerufen am 24.11.2017.
[17] Bundesministerium für Bildung und Forschung: Bewilligte Projekte aus der Bekanntmachung „Mustererkennung“, auf https://www.sifo.de/de/bewilligte-projekte-aus-der-bekanntmachung-mustererkennung-1771.html, abgerufen am 24.11.2017.
[18] Bspw. APFeL, MisPel, Muskat, Muvit, etc.

Mit der Einführung und Etablierung einer intelligenten VÜ erhofft sich der Gesetzgeber verbesserte Möglichkeiten, bei der Verhinderung von Straftaten und bei der Fahndung nach Tätern. Dadurch soll nicht zuletzt die Sicherheit in öffentlich zugänglichen Räumen gewährleistet und das Sicherheitsgefühl der Bevölkerung gestärkt werden. [19] Der primäre Einsatz durch die Sicherheits- und Strafverfolgungsbehörden verfolgt mithin auch nachgelagerte Ziele. Ob die Technik der intelligenten VÜ diesen Hoffnungen gerecht werden kann wird nachfolgend geprüft. Dabei werden mögliche operative Einsatzmöglichkeiten für die Strafverfolgungsbehörden vorgestellt und die Wirksamkeit dieser neuen Technologie in Abgrenzung zur konventionellen VÜ dargestellt. Zudem wird erörtert, ob die derzeit bestehenden Befugnisnormen in den Polizeigesetzen der Länder und des Bundes sowie der Strafprozessordnung den polizeilichen Einsatz einer intelligenten VÜ hinreichend ermöglichen oder ob eine Ausweitung der bestehenden Eingriffsermächtigungen notwendig ist. Dabei wird insbesondere darauf eingegangen, welche juristischen Hürden dafür zu überwinden sind und welche Anforderungen an eine Rechtsgrundlage gestellt werden müssen, um entsprechende Grundrechtseingriffe zu rechtfertigen.

Neben neuen Möglichkeiten können mit der Einführung einer neuen Technologie, auch Risiken verbunden sein. Neben kalkulierbaren Folgen kommt es bisweilen auch zu unerwarteten Schäden, die Gefahren oder zumindest Nachteile für einzelne Personen oder Gruppen mit sich bringen.[20] Gerade im Zusammenhang mit einer iVÜ erfährt das bekannte Dilemma Sicherheit versus Freiheit eine besondere Ausprägung.[21] Das Themenfeld der iVÜ öffentlich zugänglicher Räume lässt sich deshalb nur durch eine ganzheitliche Betrachtung der drei entscheidenden Dimensionen der Sicherheitsforschung, nämlich Technik, Recht und Gesellschaft erschließen. [22]

---

[19] Vgl. BT-Drucksache 18/10758, S. 3.
[20] Kees: Algorithmisches Panopticon, S. 32.
[21] Bergfink: Videoüberwachung im ÖPNV in Chancen und Risiken von Smart Cams im öffentlichen Raum, S. 57.
[22] Vgl. Humer: Abschlussbericht MisPel-S, S. 22.

B Begriffliche und technische Grundlagen

Im folgenden Abschnitt werden wichtige Begriffe erläutert und ein grober Überblick zu den technischen Grundlagen geschaffen.

I Die polizeiliche VÜ

Für den Begriff der Videoüberwachung gibt es keine einheitliche und abschließende Definition.[23] Sie kann aber als eine Beobachtung mit optisch-elektronischen Einrichtungen bezeichnet werden.[24] „Videoüberwachung ist ein tatsächliches Phänomen, welches verschiedene Gesetze in unterschiedlichen Formulierungen wertneutral und auf den technischen Vorgang abzielend umschreiben und präzisieren."[25] So unterscheiden einige Landespolizeigesetze explizit die „Beobachtung" von der „Aufzeichnung"[26]. Andere Gesetze hingegen kennen nur den Begriff der Videoaufzeichnung, hier wird das reine „Beobachten" lediglich als Mindermaßnahme verstanden.[27]

Die polizeiliche VÜ des öffentlichen Raumes kann mit unterschiedlichen Zielsetzungen durchgeführt werden. Sie kann als präventives Instrument angesehen werden, wenn der Einsatz der Technik der Verhinderung von Straftaten bspw. an Kriminalitätsbrennpunkten dient. Sie kann aber auch als ein Instrument der Repression angesehen werden, wenn sich der Aufzeichnung eine strafrechtliche Auswertung anschließt.[28] Exemplarisch wird insoweit die Doppelnatur polizeilicher Aufgaben deutlich; die Gewährleistung der öffentlichen Sicherheit und Ordnung sowie die Erfüllung von Aufgaben der Strafverfolgung.

Die überwiegende Meinung in der Literatur sieht die VÜ als Oberbegriff für beide Vorgänge. Der Begriff lasse keine Unterscheidung zwischen Beobachten und Aufzeichnen zu oder impliziere ein bestimmtes Ziel.[29] Nachfolgend

---

[23] Vgl. Maximini: Polizeiliche Videoüberwachung, S. 4.
[24] Vgl. § 6b BDSG; vgl. Voß: Videoüberwachung im öffentlichen Raum auf http://www.krimlex.de/artikel.php?BUCHSTABE=V&KL_ID=225, abgerufen am 24.11.2017.
[25] Held: Intelligente Videoüberwachung, S. 20.
[26] Vgl. Starnecker: Videoüberwachung zur Risikovorsorge, S. 25.
[27] Vgl. Brenneisen/Staack: Die Videobildübertragung nach allgemeinem Polizeirecht, S. 449.
[28] Vgl. Voß: Videoüberwachung im öffentlichen Raum auf http://www.krimlex.de/artikel.php?BUCHSTABE=V&KL_ID=225, abgerufen am 24.11.2017.
[29] Vgl. Held: Intelligente Videoüberwachung, S. 20; vgl. Starnecker: Videoüberwachung zur Risikovorsorge, S. 25; vgl. Maximini: Polizeiliche Videoüberwachung, S. 5.

wird der Begriff der VÜ synonym für die Beobachtung und die Aufzeichnung verwendet, außer eine andere Bedeutung wird explizit benannt.

II Öffentlich zugängliche Räume

Der Begriff „öffentlicher Raum“ kann unterschiedlich definiert werden. Für die nachfolgende Betrachtung ist eine Unterscheidung im eigentumsrechtlichen Sinne weniger signifikant. Vielmehr soll die soziale Begegnung und die Zugänglichkeit des öffentlichen Raums im Fokus stehen.[30] Nach *Klauser* ist darunter der „zugängliche und nutzbare, in Idealform gesellschaftlich geteilte Raum“[31] zu verstehen. Entscheidend ist nach dieser Ansicht, dass in diesem Raum das gesellschaftliche Leben stattfindet und auch private, aber dennoch für die Allgemeinheit zugängliche Räume, wie Bahnhöfe und öffentliche Bereiche von Flughäfen, darunter fallen.[32] Nach § 6b BDSG sind sie als „räumlichen Bereiche zu verstehen, die von einem unbestimmten oder nur nach allgemeinen Merkmalen bestimmten Personenkreis betreten und genutzt werden können und dazu auch bestimmt sind. Der Bereich kann innerhalb oder außerhalb eines Gebäudes liegen“.[33] Entscheidend ist, ob es sich entweder nach der Zweckbestimmung oder der Widmung des Berechtigten um Bereiche handelt, die der Allgemeinheit zugänglich sind.[34]

Die VÜ öffentlich zugänglicher Bereiche unterscheidet sich in Struktur und Ziel von der Überwachung des nichtöffentlichen Raums.[35] Sie verfolgt einen normativen Ansatz.[36] Der Fokus der konventionellen Videoüberwachung ist nicht das Individuum, sondern der zu überwachende Ort.[37] Diese Abgrenzung ist für die Zuordnung der Ermächtigungsgrundlagen für den Einsatz polizeilicher VÜ

---

[30] Vgl. Klauser: Die Videoüberwachung öffentlicher Räume, S. 138.
[31] Ebd. S. 164.
[32] Kees: Algorithmisches Panopticon, S. 21; Andere Meinung: Glatzner: Die staatliche Videoüberwachung des öffentlichen Raumes, S. 6.
[33] Vgl. Bergmann/Möhrle/Herb: BDSG, § 6b, Rn. 8.
[34] Vgl. OVG Lüneburg, ZD 2014,636; vgl. Lee/Reirach: Einsatz von Body Cams bei privaten Sicherheitsdiensten in Chancen und Risiken von Smart Cams im öffentlichen Raum, S. 217.
[35] Vgl. Kees: Algorithmisches Panopticon, S. 21.
[36] Vgl. Klauser: Die Videoüberwachung öffentlicher Räume, S. 71.
[37] Vgl. ebd., S. 91.

von wesentlicher Bedeutung. Obwohl VÜ ein Instrument der Raumkontrolle ist, hat sie Einfluss auf das Individuum und die Gesellschaft.[38]

III Intelligente VÜ

Üblicherweise erfolgt die konventionelle Videoüberwachung nach dem Kamera-Monitor-Prinzip, bei dem die Videobilder auf einen Monitor oder ein Aufzeichnungsgerät übertragen werden und durch eine natürliche Person in Echtzeit oder retrograd ausgewertet werden.[39]

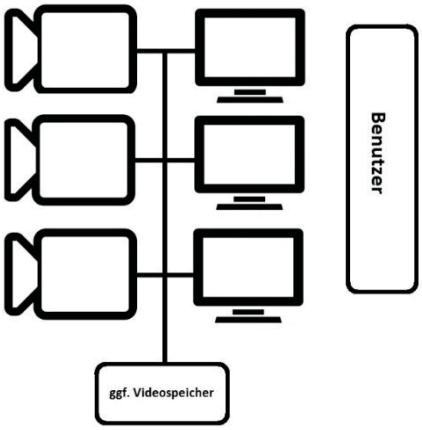


Abbildung 1: Systemarchitektur konventioneller Videoüberwachung[40]

Analog zur konventionellen VÜ ist der Begriff der „intelligenten VÜ" (engl. smart CCTV) nicht klar definiert.[41] Schon der Begriff „Intelligenz" zählt zu den umstrittensten Begriffen im Bereich der Philosophie und Ethik.[42] Nach *Held* gilt Videoüberwachungstechnik als intelligent, wenn sie mindestens eine Mustererkennungsfunktion aufweist. Die drei wesentlichen Verfahren sind insoweit das Erkennen und Verfolgen von Objekten und Personen, die Analyse von Verhaltensmustern sowie die Erkennung von Gesichtern.[43] Den entscheidenden Schritt von der konventionellen zur intelligenten Videoüberwachung erfährt das Überwachungssystem dadurch, dass es „selbst die Bilder in Echtzeit

---

[38] Vgl. Kees: Algorithmisches Panopticon, S. 22.
[39] Vgl. Brenneisen/Staack: Die Videobildübertragung nach allgemeinem Polizeirecht, S. 447; Bretthauer: Intelligente Videoüberwachung, S. 35.
[40] Angelehnt an Held: Intelligente Videoüberwachung, S. 26.
[41] Vgl. Held: Intelligente Videoüberwachung, S. 21.
[42] Vgl. Wolkenstein: Intelligente Videoüberwachung aus ethischer Perspektive, S. 25.
[43] Vgl. Held: Intelligente Videoüberwachung, S. 21.

auswerten kann“[44] und die Videoanalyse und -interpretation ohne menschliches Personal von statten geht.[45] Diese zielgerichtete Analyse und Bewertung von Informationen durch ein technisches System soll Objekte und räumliche Veränderungen erkennen können und menschliches Verhalten überwachen. Ursprung dieser Informationen können eine oder mehrere Quellen (Kameras) sein, die unabhängig voneinander oder miteinander verknüpft sind. IVÜ ist somit der Einsatz von Videoanalyse und automatisierten Datenabgleich.[46]

Technisch funktioniert die intelligente Videoüberwachung aufgrund eines sog. „ASIP-Blocks“, der für die Analyse und Auswertung der durch die optische Linse aufgenommenen Bilder verantwortlich ist. Diese technische Einheit ist ein Mikroprozessor, der mit einer Software ausgestattet ist, die je nach Algorithmus Bilder analysiert, Informationen extrahiert, Muster erkennt, Ereignisse detektiert und gegebenfalls Entscheidungen trifft.[47] Dabei ist es grundsätzlich unerheblich, ob diese Bildanalyse direkt in der Kamera oder durch einen Computer gestützte Auswertung stattfindet. Beide Verfahren weisen spezifische Vor- und Nachteile auf, die je nach Projekt und Anforderung des Anwenders abgewogen werden müssen.[48]

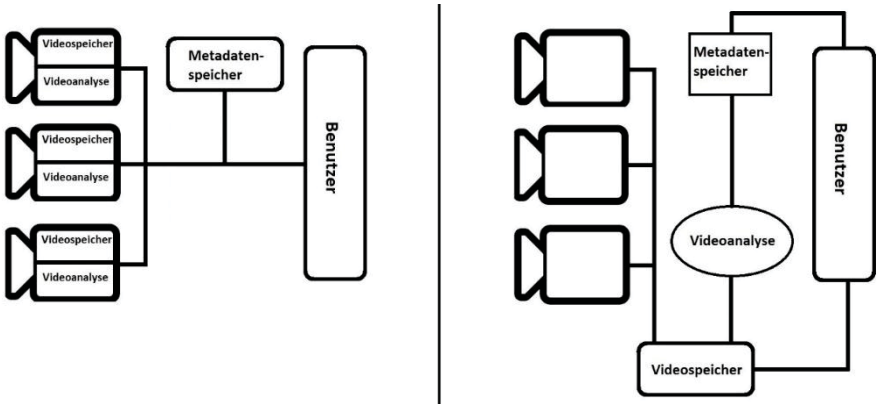


Abbildung 2: Systemarchitektur einer dezentralisierten (Variante a) bzw. einer zentralisierten (Variante b) intelligenten Videoüberwachung[49]

---

[44] Vgl. Held: Intelligente Videoüberwachung, S. 21.
[45] Vgl. Bretthauer: Intelligente Videoüberwachung, S. 35.
[46] Vgl. Bretthauer: Intelligente Videoüberwachung, S. 37; vgl. Müller: Videoüberwachung in öffentlich zugänglichen Räumen, S. 17; vgl. Vagts: Privatheit und Datenschutz in der intelligenten Überwachung, S. 11.
[47] Vgl. Bretthauer: Intelligente Videoüberwachung, S. 38f.
[48] Anstädt/Keller/Lutz: Intelligente Videoanalyse, S. 29.
[49] Angelehnt an Held: Intelligente Videoüberwachung, S. 26f.

1. Video-Tracking

Video-Tracking ist im weitesten Sinne die Grundfunktion der Analyse, denn Tracking ist jedes visuelle Abtasten der Position (Objektdetektion) und Bewegung eines Objektes (bzw. Subjekts) im „Sichtbereich" der optischen Aufnahmeeinrichtung. Es ist somit nötig für die Erkennung und Klassifikation eines Objektes. Im engeren Sinn bedeutet Tracking aber auch die Verfolgung eines Objektes bzw. einer Person. Die optische Verfolgung einer Person durch eine Szenerie kann dabei durch eine oder mehrere Kameras erfolgen und raumübergreifend stattfinden. Letzteren falls wird das zu beobachtende Objekt gewissermaßen weitergereicht.[50] Das optische Verfolgen oder „Tracken" von Personen durch mehrere Kameras stellt an die technische Realisierung hohe Ansprüche, da die Personen durch Gegenstände und andere Personen verdeckt werden können. Ebenso können sich die Ausgangssituationen, wie Lichteinfall und Helligkeit, ändern und das Personenverhalten individuell variiert.[51] Über die Verfolgung hinaus kann durch die eingesetzte Software ein Bewegungsprofil erstellt werden. Dieser weitergehende Schritt fällt begrifflich bereits unter die Mustererkennung.[52]

2. Mustererkennung

Unter Mustererkennung im Sinne einer iVÜ kann die Erfassung und automatisierte Verarbeitung von optisch gewonnen Daten verstanden werden, die die Suche nach Strukturen, wie Regelmäßigkeiten, Wiederholungen, Ähnlichkeiten oder Gesetzmäßigkeiten zum Ziel hat. Im Sinne einer polizeilichen (intelligenten) VÜ sind darunter alle Systeme, die für eine präventive und repressive Kriminalitätsbekämpfung konzipiert wurden, zu verstehen.[53] Als wesentliche Analysemethoden der Mustererkennung in der Sicherheitstechnologie sind die Objektdetektion, die biometrische Erkennung und die Verhaltenserkennung zu

---

[50] Vgl. Bretthauer: Intelligente Videoüberwachung, S. 40; vgl. Held: Intelligente Videoüberwachung, S. 22.
[51] Fillbrandt: Videobasiertes Multi-Personentracking in komplexen Innenräumen, S. 7.
[52] Vgl. Bretthauer: Intelligente Videoüberwachung, S. 40.
[53] Vgl. Held: Intelligente Videoüberwachung, S. 22.

nennen. Nachfolgend sollen diese Analyseverfahren an konkreten Einsatzmöglichkeiten dargestellt werden. Unterschieden wird dabei in Mustererkennung mit und ohne Personenbezug.

C Aktueller Stand der technischen Entwicklung und Funktionsweisen der verschiedenen Systeme

Der nachfolgende Abschnitt zeigt die verschiedenen Varianten von Analysesystemen auf. Hierfür wird der derzeitige Stand der technischen Entwicklung anhand ausgewählter Verfahren und Projekte vorgestellt.

I Objektdetektion und -erkennung

Die Objektdetektion ermöglicht es, Veränderungen in einem vordefinierten Bereich des Videobildes automatisch zu erkennen.[54] Je nach eingesetztem Algorithmus kann sie erkennen, ob ein Objekt hinzugetreten ist oder entfernt wurde. Diese Technik wird vor allem zur Überwachung von Gegenständen in Museen oder Kaufhäusern eingesetzt.[55] Die Objekterkennung hingegen ermöglicht zusätzlich die Identifizierung von unterschiedlichen Gegenständen und deren Abgrenzung von Personen.[56] Der polizeiliche Einsatz der Objekterkennung ist weit gefächert. So sind diese Systeme in der Lage zurückgelassenes Gepäck aufzuspüren, welches bei kritischen Infrastrukturen zunächst grundsätzlich als NZG eingestuft wird. Erst durch einschreitende Sicherheitskräfte wird indes Verifizierung vorgenommen, ob es sich um eine harmlose Fundsache handelt oder um einen „Bombenkoffer".[57] Auch das Erkennen von Personen in gesperrten bzw. Gefahrenbereichen ist eine denkbare Anwendungsmöglichkeit eines solchen Algorithmus.[58]

Seit über zehn Jahren wird bereits von einigen Bundesländern die automatisierte Erkennung amtlicher Kfz-Kennzeichen zur Gefahrenabwehr eingesetzt.[59] Dabei wird von einer Überwachungskamera das Kennzeichen erfasst

---

[54] Vgl. Müller: Videoüberwachung in öffentlich zugänglichen Räumen, S. 17.
[55] Vgl. Bretthauer: Intelligente Videoüberwachung, S. 40.
[56] Vgl. ebd., S. 40.
[57] Vgl. Anstädt/Keller/Lutz: Intelligente Videoanalyse, S. 61.
[58] Vgl. Held: Intelligente Videoüberwachung, S. 25.
[59] Vgl. ebd., S. 22.

und durch einen Algorithmus lokalisiert, aufbereitet und die einzelnen Buchstaben und Ziffern für die Software lesbar gemacht. Anschließend findet ein automatisierter Abgleich der Daten mit dem Fahndungsbestand statt.[60] Erst bei einem Treffer verständigt das System einen Operator (Polizeibeamten/-innen), der dann weitere Maßnahmen trifft.

Das Beispiel der automatischen Kennzeichenerkennung zeigt, dass der polizeiliche Einsatz von Videoüberwachung mit „intelligenten" Systemen keine Utopie, sondern zumindest in einigen Bundesländern seit Jahren, gängige Praxis ist. Das Lesen eines Nummernschildes ist mit den heutigen technischen Möglichkeiten keine Hürde mehr. Diese Art der Objekterkennung ist dennoch nur ein kleiner Teil der Möglichkeiten, die aus technischer Sicht realisierbar sind. Hinsichtlich der Kennzeichen-Erkennung ist für die Sicherheitsbehörden zwar ein Nutzen erkennbar, dieser lässt sich jedoch nicht immer realisieren. In Bayern werden beispielsweise jährlich etwas acht Millionen Kfz-Kennzeichen erfasst, dabei registrierten die Geräte zwischen 50 000 und 60 000 Übereinstimmungen in den Datenbanken. Erst im Anschluss glich ein Polizeibeamter manuell das tatsächliche Bild mit dem Datenbankeintrag ab. Es stellte sich heraus, dass nur 500 bis 600 der erfassten Bilder, also etwa ein Prozent ein Fahndungstreffer waren.[61] Schließlich führen auch diese positiven Treffer in einer Fahndungsdatenbank nicht automatisch zu einem Einschreiten der Beamten und somit zu einer entsprechenden Maßnahme.

Moderne Kameras und ausgefeilte Algorithmen können heute allerdings nicht nur einzelne Objekte detektieren, sondern greifen auch auf einen Fundus von Referenzobjekten zurück und helfen so, unterschiedliche Objekte automatisch zu klassifizieren. Der Einsatz dieser Analysemöglichkeiten findet derzeit noch nicht im realen Wirkbetrieb statt, da die rechtlichen Grundlagen für eine solche Videoanalyse für die Polizei bislang nicht klar definiert sind.

---

[60] Vgl. Schieder: Die automatisierte Erkennung amtlicher Kfz-Kennzeichen, S. 778; vgl. Kilchling/Kenzel: Recht und Praxis der anlassbezogenen automatischen Kennzeichenfahndung, Verkehrsdatenabfrage und Mobilfunkortung zur Gefahrenabwehr in Brandenburg, S. 24f.

[61] Haberl: Automatische Kennzeichenerkennung, auf http://www.sueddeutsche.de/auto/automatische-kennzeichenerkennung-wo-ihr-nummernschild-erfasst-wird-1.2188409, abgerufen am 03.12.2017.

II Biometrische Erkennung

Das Ziel der biometrischen Erkennung durch Videoüberwachung ist, die Identität einer Person zu ermitteln (Identifikation). Etymologisch ist Biometrie die Technik der Erkennung einer Person mittels persönlicher Charakteristika.[62] Die biometrische Erkennung erfolgt anhand messbarer, individueller körperlicher Merkmale einer Person. Neben einzelnen Körperteilen, wie Augen, Ohren, Gesicht, Händen und Finger (Daktyloskopie) eignen sich u. a. die Besonderheiten der Stimme und der Verhaltensweisen, wie bspw. die Gangart, zur Identifikation.[63]

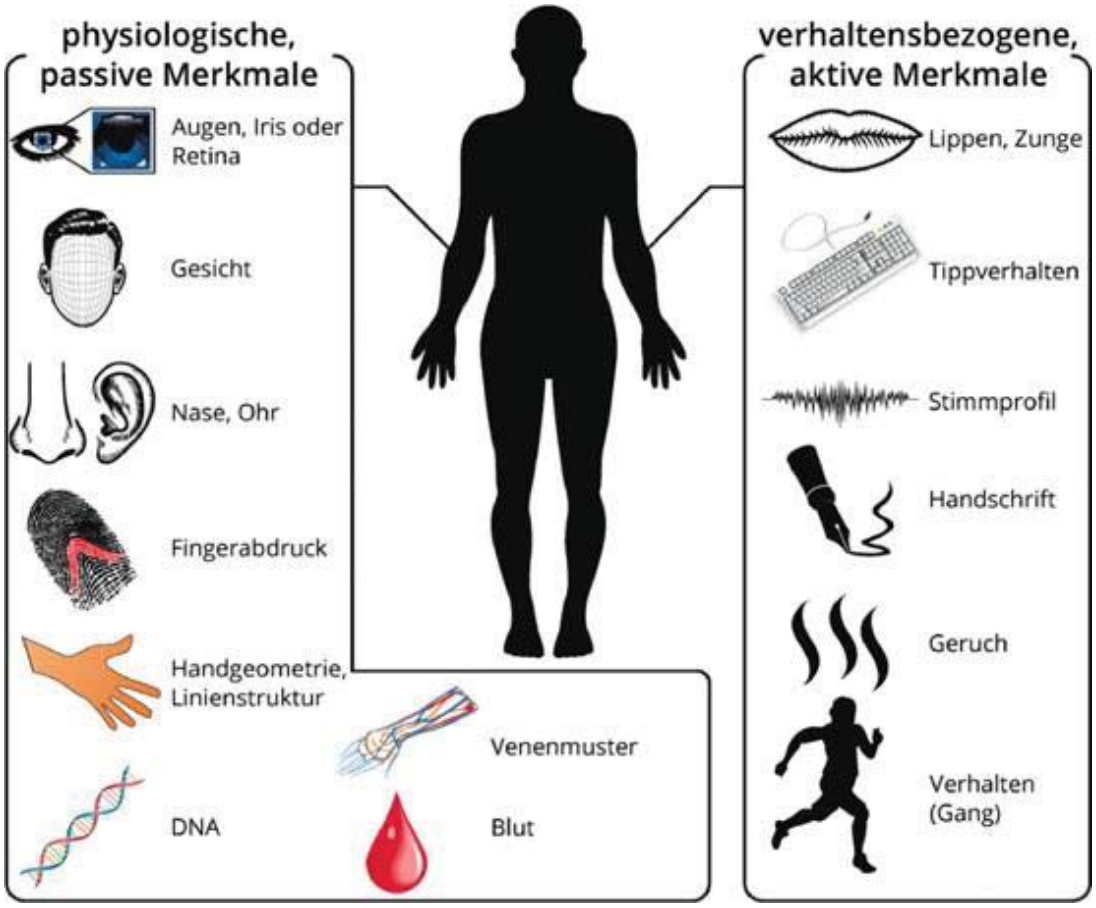


Abbildung 3: Darstellung einer möglichen Einteilung biometrischer Merkmale auf der Grundlage ihrer Entstehung und Veränderbarkeit. Es werden die Gruppen der physiologischen bzw. verhaltensbezogenen Merkmale unterteilt.[64]

---

[62] Bundesamt für Sicherheit in der Informationstechnik: Grundsätzliche Funktionsweise biometrischer Verfahren auf https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/Biometrie/AllgemeineEinfuehrung/einfuehrung.html, abgerufen am 06.12.2017.
[63] Vgl. Meuth: Zulässigkeit von Identitätsfeststellungen mittels biometrischer Systeme durch öffentliche Stellen, S. 18.
[64] Labudde: Biometrie und die Analyse digitalisierter Spuren, S. 32.

In der Literatur[65] werden für die Bewertung eines Merkmals hinsichtlich seiner Eignung für die biometrische Identifikation die folgenden Anforderungen formuliert:

- Universalität, d.h. ein Merkmal ist bei jeder Person vorhanden,
- Einzigartigkeit, d.h. ein Merkmal ist bei jeder Person anders,
- Permanenz, d.h. ein Merkmal ist zeitlich invariant,
- Erfassbarkeit, d.h. ein Merkmal lässt sich quantitativ erheben.[66]

Aus dieser Aufstellung lassen sich die Vorteile einer Identifikation anhand biometrischer Merkmale ableiten nämlich „dass sie personengebunden, in der Anzahl begrenzt und in der Regel nicht geheim sind".[67] Ganz im Gegenteil zu körperlichen Merkmalen, wie das Gesicht, welches offen für jedermann zu sehen ist. Zudem können biometrische Merkmale nicht übertragen oder weitergegeben werden. Ist die „Zuordnung des körperlichen Merkmals zu einer Person korrekt erfolgt, kann mit Verwendung dieses Merkmals [..] sichergestellt werden, dass es sich bei der vorhandenen Person tatsächlich um die angenommene bzw. behauptete Identität handelt."[68] Der Ablauf einer biometrischen Erkennung folgt bei allen Systemen dem gleichen Grundprinzip. Im ersten Schritt muss die zu identifizierende Person im System angelegt werden (Enrolment). Hierfür eigenen sich Fotos bzw. Standbilder aus Videoaufnahmen. Es gilt der Grundsatz, je besser die Bildqualität (Auflösung, Schärfe, Helligkeit), desto höher die spätere Wahrscheinlichkeit einer Zuordnung. Im nächsten Schritt erfolgt die Erfassung der biometrisch relevanten Eigenschaften einer Person, z.B. des Gesichts. Daraus werden Referenzdatensätzen (Templates) erstellt und der angelegten (unbekannten) Person zugewiesen. Neben den aus den Rohdaten erstellten Templates sollten die Rohdaten selbst

---

[65] Vgl. Jain/Bolle/Pankanti: Biometrics, S.4.
[66] Reimer: Biometrische Identifikation in Biometrische Identifikation, S. 11.
[67] Ebd. S. 19.
[68] Vgl. Bundesamt für Sicherheit in der Informationstechnik: Grundsätzliche Funktionsweise biometrischer Verfahren auf https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/Biometrie/AllgemeineEinfuehrung/einfuehrung.html, abgerufen am 06.12.2017.

ebenfalls gespeichert werden, damit die Originaldaten für eine weitere manuelle Auswertung zur Verfügung stehen.[69] Nachdem die Person mit ihrem individuellen Merkmalssatz im System erfasst wurde, kann sie beim sog. Matching mit einem weiteren Datensatz (Fahndungsbestand, weiteres Videomaterial, etc.) abgeglichen werden.[70]

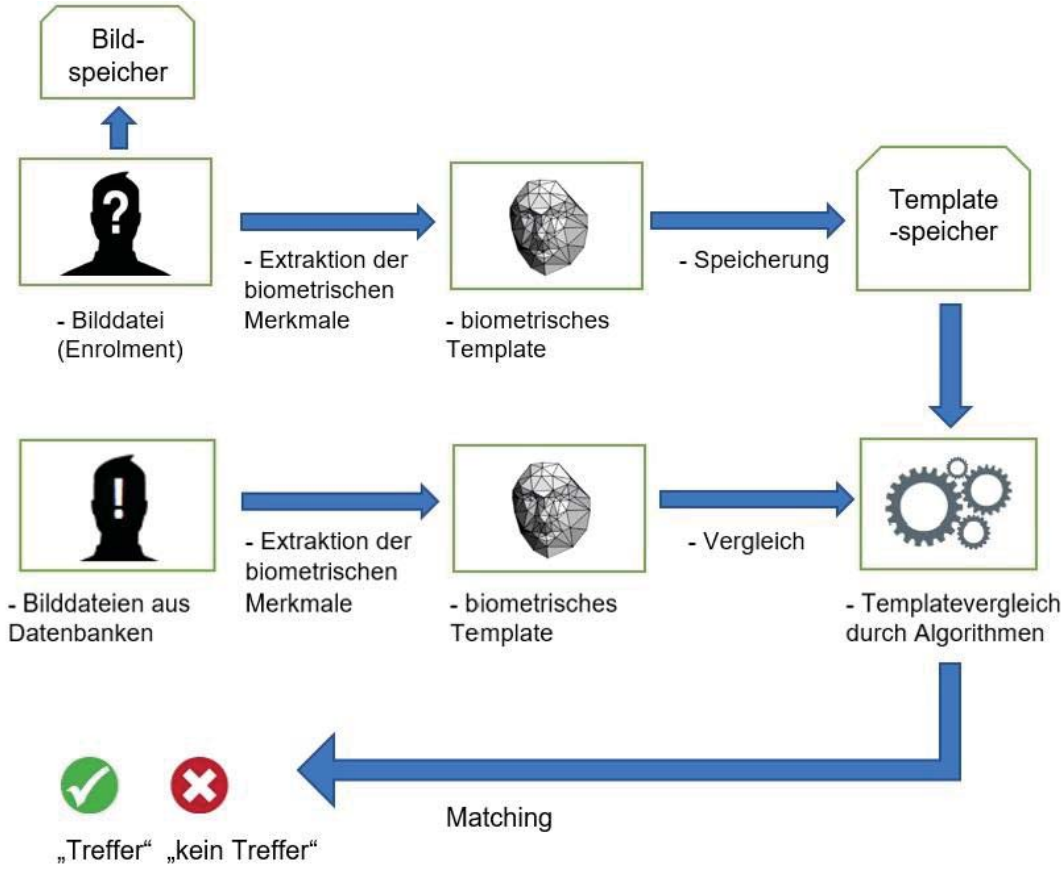


Abbildung 4: Typischer Systemaufbau für eine biometrische Identifikation[71]

Eine polizeiliche Videoüberwachung, die eine biometrische Erkennung vornimmt, hat die unmittelbare und vor allem kontaktlose Identifizierung einer Person zum Ziel. Dies schränkt die Möglichkeiten der Nutzung persönlicher Charakteristika ein. Gemessen an den vier Bewertungskriterien zur Eignung eines

[69] Vgl. Meuth: Zulässigkeit von Identitätsfeststellungen mittels biometrischer Systeme durch öffentliche Stellen, S. 23.
[70] Vgl. ebd, S. 20f, vgl. Bundesamt für Sicherheit in der Informationstechnik: Grundsätzliche Funktionsweise biometrischer Verfahren auf https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/Biometrie/AllgemeineEinfuehrung/einfuehrung.html, abgerufen am 06.12.2017.
[71] Angelehnt an Weber: Gesichtserkennung in Biometrische Identifikation, S. 112.

Merkmals kann festgestellt werden, dass kein biometrisches Merkmal alle Kriterien erfüllt.[72] Die Gesichtserkennung stellt indes den Schwerpunkt der Forschung im Bereich der biometrischen Verfahren im Sicherheitsbereich dar. Neben den zahlreichen messbaren Besonderheiten, die Gesichter weltweit aufweisen, sind die Anwendungsmöglichkeiten der Gesichtserkennung hierfür auschlaggebend.[73]

Bereits seit 2008 nutzt das BKA Gesichtserkennungssoftware (GES 2D/3D)[74] zur Suche nach Übereinstimmungen in der INPOL-Datenbank.[75] Dort sind rund vier Millionen Lichtbilder eingestellt, die mit biometrischen Verfahren durchsucht werden können. Hierbei können mittels automatisiertem Lichtbildvergleich Personenidentifikationen vorgenommen werden. Es werden zwar nur Bilddateien verarbeitet, diese können aber durchaus aus Standbildern von Videodaten stammen.[76] Im Kalenderjahr 2016 wurden so über 23.000 Recherchen im zentralen Gesichtserkennungssystem durchgeführt.[77] Das Verfahren ist relativ zeitintensiv und ist für eine Echtzeitanalyse ungeeignet. Die technischen Möglichkeiten, die mit der Gesichtserkennungssoftware GES 3D geschaffen wurden dienten weiteren Projekten als Grundlage. Das Verbundprojekt MisPel beispielsweise hatte zum Ziel Möglichkeiten zu entwickeln, um eine forensische Analyse großer Datenmengen schnell und effizient durchzuführen. Dies sollte anhand der Recherche von „Bild- und Videomaterial unter Nutzung gesichtsbasierter biometrischer und soft-biometrischer Merkmale“[78] geschehen. „In diesem Vorhaben […] standen u.a. die folgenden Szenarien im Vordergrund:

- Suche nach einer Person in Videomassendaten auf Grundlage eines vorgegebenen (Fahndungs-)Fotos
- Extraktion eines Gesichts aus Videodaten zwecks Abgleich mit Lichtbilddatenbanken

---

[72] Vgl. Meuth: Zulässigkeit von Identitätsfeststellungen mittels biometrischer Systeme, S. 27.
[73] Vgl. ebd., S. 26.
[74] BT-Drucksache 18/8492, S. 7.
[75] INPOL ist das gemeinsame Informationssystem aller Polizeibehörden in Deutschland.
[76] Vgl. Monroy: BKA schließt Probelauf zur Gesichtserkennung ab, S. 1.
[77] Vgl. BT-Drucksache 18/13205, S. 9.
[78] Stiefelhagen: Abschlussbericht MisPel, S. 2.

- Vergleich von Personendaten aus unterschiedlichen Videoquellen
- Nutzung softbiometrischer Beschreibungen wie Kleidung, Gang, etc. für die Personensuche."[79]

Die im Projekt MisPel gewonnenen Erkenntnisse zur Personenidentifikation unter Nutzung einer automatischen Gesichtserkennung, die auf polizeiliche Daten anwendbar wäre, waren vielversprechend und stellten nach Meinung der Forscher „einen notwendigen Schritt auf dem Weg zur Entwicklung eines innovativen Produkts dar".[80] Derzeit läuft das Projekt „Sicherheitsbahnhof am Berliner Südkreuz", das eine Gesichts- und Verhaltenserkennung im realen Wirkungsbetrieb eines Bahnhofes testen soll.[81]

III Tracking und Verhaltenserkennung

Mit der Analyse von Personenbewegungen an Flughäfen mittels zeitlich rückwärts- und vorwärtsgerichteter Videodatenströme befasste sich das Projekt APFel. Ziel hierbei war es, eine zuvor von einem Operator markierte, sich verdächtig benehmende Person über mehrere Kameras hinweg verfolgen zu können. Durch eine sogenannte Vorwärtsanalyse sollte der wahrscheinlichste zukünftige Weg, der Person vorhersagt werden können und mittels Rückwärtsanalyse sollten die bisher zurückgelegten Wege verfolgt werden können. Hiervon verspricht man sich eine frühzeitige Einschätzung und Eindämmung des Gefahrenpotenzials von verdächtigen Personen.[82] Ebenfalls mit dem „Tracking" von Personen, wenngleich mit anderen Zielsetzungen, befassten sich die Projekte MuViT und Muskat.

Der Forschungsbereich der Verhaltenserkennung reicht von der Analyse einer bewegungslosen und somit potenziell hilflosen Person bis hin zum Erkennen komplexer Situationen (Erkennen einer Angriffs- bzw. Kampfsituation[83] oder

---

[79] Eigenseer/Humer/Lederer: Von der konventionellen zur intelligenten Videoüberwachung in Digitale Polizeiarbeit, S. 148.
[80] Stiefelhagen: Abschlussbericht MisPel, S. 18.
[81] Vgl. Biselli: „Projekt Sicherheitsbahnhof", S. 1.
[82] Feltes/Kudlacek/Ruch: Schlussbericht zum Verbundprojekt: Analyse von Personenbewegungen an Flughäfen mittels zeitlich rückwärts- und vorwärtsgerichteter Videodatenströme (APFel), S. 3.
[83] Vgl. Anstädt/Keller/Lutz: Intelligente Videoanalyse, S. 68.

von „abweichendem Verhalten“[84]). Je komplexer das zu analysierende Verhalten, desto unausgereifter und ineffizienter sind die technischen Systeme. So stellt das Erkennen einer liegenden Person mittlerweile kein Problem mehr dar, die Analyse und Bewertung, ob von einer Person eine Gefahr ausgehen könnte hingegen schon. Diese Kategorisierung nennt man Profiling. „Profiling besteht aus den komplementären (Handlungs-) Prozessen der Erstellung von Kategorien und der Einordnung von Entitäten in diese Kategorien zur Ableitung neuer handlungsrelevanter Informationen. Es beinhaltet die Elemente der Differenzierung, der Generalisierung und der Vorhersage.“[85] Diese Bandbreite stellt schon an menschliche Akteure im Sicherheitsbereich enorme Anforderungen[86] mit unterschiedlichen Ergebnissen und ist aufgrund der Komplexität menschlicher Verhaltensweisen für einen Algorithmus schwer zu analysieren.

IV Zusammenfassung

Es gibt nicht *die* intelligente Videoüberwachung. Es sind vielmehr verschiedene Varianten von Analysesystemen. Die Einführung der Objektdetektion und -analyse zur automatischen Kennzeichenerfassung war der erste Schritt, um intelligente Videoüberwachung für das polizeiliche Tätigkeitsfeld nutzbar zu machen. Der Forschungsschwerpunkt ist derzeit in der Gesichtserkennung und der Suche nach Personen in Videomassendaten zu sehen. Dabei spielt es aus technischer Sicht weniger einer Rolle, ob dies zum Abgleich mit Datenbanken, bspw. bei Personenfahndung oder zum Verfolgen einer Person über mehrere verschiedene Kamerasysteme (Tracking) geschieht. Auch wenn aus Sicht der Auftraggeber und Forscher die technischen Ergebnisse der Projekte zumindest im Labor überzeugt haben, so sollte die Einführung und Weiterentwicklung einer solchen intelligenten VÜ für polizeiliche Zwecke immer unter Einbindung des Endanwenders stattfinden. Neben operativen Einsatzmöglichkeiten muss auch eine kriminalistische Wirkung nachweisbar sein. Weiterhin müssen die rechtlichen Schranken eingehalten werden.

---

[84] Vgl. Held: Intelligente Videoüberwachung, S. 164.
[85] Schäufele: Profiling zwischen sozialer Praxis und technischer Prägung, S. 11.
[86] Vgl. Grochwski: Aktuelle Praxis und Implikationen zur Identifikation von Attentätern, S. 25.

D Operative Einsatzmöglichkeiten „intelligenter“ VÜ aus polizeilicher Sicht

Technische Hilfsmittel wie die konventionelle VÜ erleichtern und effektivieren sowohl die präventive als auch die repressive Polizeiarbeit.[87] Die polizeiliche VÜ des öffentlichen Raums wurde in Deutschland ursprünglich vor allem als kriminalpräventives Instrument eingeführt.[88] Alle Polizeigesetze der Länder[89] und der Bundespolizei enthalten eine Befugnisnorm zum „Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufzeichnungen.“[90] Die VÜ öffentlich zugänglicher Räume gehört rechtsdogmatisch gesehen zur sogenannten „Gefahrenvorsorge.“[91] Sie dient dazu, die ureigenste Aufgabe der Polizei – die Gefahrenabwehr – mit Sachmitteln zu unterstützen. Kriminalpolitisch ist sie Teil der sekundären Prävention und soll unmittelbar auf den Täter bzw. die Tatsituation einwirken und aus Täter Sicht negativ beeinflussen.[92] Auch in der Strafverfolgung wird die VÜ bspw. zur Fahndung oder als Sachbeweis im Strafverfahren genutzt.[93] Sie kann somit auch ein Teil der Kriminaltechnik sein.

Die VÜ ist für sich genommen ein unbrauchbares Mittel, solange das übertragene bzw. aufgezeichnete Videobild nicht gesichtet und ausgewertet wird sowie weitere Maßnahmen veranlasst werden. Dies ist jedoch sehr zeit- und personalintensiv, weshalb nicht jedes aufgeschaltete Kamerabild durch einen Menschen beobachtet wird. Diesem Umstand könnte die Analysefunktion der intelligenten VÜ entgegenwirken. Die in Kapitel C skizzierten Funktionsweisen zeigen, dass die intelligente VÜ eine enorme Arbeitserleichterung durch gleichzeitige Einsparung von personellen und zeitlichen Ressourcen für die Polizei bedeuten kann.

---

[87] Vgl. Bartsch: Rechtsvergleichende Betrachtung präventiv-polizeilicher Videoüberwachungen öffentlich zugänglicher Orte in Deutschland und in den USA, S. 34.
[88] Vgl. Glatzner: Die staatliche Videoüberwachung des öffentlichen Raumes, S. 16.
[89] Eine Übersicht der Ermächtigungsgrundlagen findet sich auf: https://www.bundestag.de/blob/507980/bf8a67c2440522ac5a1ed22dd7164e66/wd-3-045-17-pdf-data.pdf, Stand 12/2017, S. 4f; Held: Intelligente Videoüberwachung, S. 38.
[90] § 15 PolG NRW.
[91] Vgl. Maximini: Polizeiliche Videoüberwachung öffentlicher Straßen und Plätze zur Kriminalitätsprävention, S. 7.
[92] Vgl. ebd., S. 8.
[93] Vgl. Voß: Videoüberwachung im öffentlichen Raum auf http://www.krimlex.de/artikel.php?BUCHSTABE=V&KL_ID=225.

I Örtlichkeiten polizeilicher Anwendung einer intelligenten VÜ

Für den Einsatz der konventionellen Videoüberwachung des öffentlichen Raums sind in den Polizeigesetzen der Länder vier Fallgruppen von Ermächtigungsgrundlagen zu unterscheiden. Demnach darf die Polizei bei öffentlichen Veranstaltungen, an gefährdeten Orten[94], bei gefährdeten Objekten und mit sogenannten „Bodycams“ Videoüberwachungsmaßnahmen ergreifen.

Die Bundespolizei darf darüber hinaus am Amtssitz eines Verfassungsorgans oder eines Bundesministeriums, an der Grenze und an kritischer Infrastruktur, wie der Anlage oder Einrichtung der Eisenbahnen des Bundes und einer dem Luftverkehr dienenden Anlage oder Einrichtung eines Verkehrsflughafens, VÜ-Maßnahmen tätigen.[95] Weitere Ermächtigungsgrundlagen für die VÜ, meist ohne örtliche Beschränkung, finden sich in einigen Versammlungsgesetzen der Länder und des Bundes sowie der Strafprozessordnung.

Der Einsatz einer intelligenten VÜ richtet sich grundsätzlich analog nach demjenigen konventioneller VÜ. Auch hier muss zur Wahrung der Grundrechte und zur Einhaltung der Rechtsprechung eine räumliche bzw. anlassbezogene Grenze gezogen werden.[96] In Betracht kommen insbesondere öffentliche Veranstaltungen und Ansammlungen, wie etwa Sportveranstaltungen oder Volksfeste. Gemessen an den taktischen Erwägungen zum Einsatz dieser Technik sind gefährliche Orte ebenso relevant. Gefährlich bzw. verrufen ist ein Ort dann, wenn aufgrund kriminalistischer Erfahrung und anderer Erkenntnisse bekannt ist, dass sich dort Straftäter aufhalten, Personen zu Straftaten verabreden, sie vorbereiten oder begehen oder dass dort der Prostitution nachgegangen wird.[97] Aber auch gefährdete Objekte und hier insbesondere die kritische Infrastruktur, wie die Versorgungs- und Verkehrseinrichtungen (öffentliche Verkehrsmittel), könnten durch den Einsatz einer intelligenten VÜ besser geschützt werden.

---

[94] Richtiger wohl: „gefährliche“ Orte, vgl. Petri: Handbuch des Polizeirechts, Rn. 215.
[95] Vgl. §§ 27; 23 Abs. 1 Nr. 4 BPolG.
[96] Näher im Kapitel F - Zulässigkeit und Legitimation.
[97] Vgl. Drewes/Malmberg/Walter: Bundespolizeigesetz, §23, Rn. 34, S. 380.

II Mögliche Einsatzszenarien

Wie auch die konventionelle polizeiliche VÜ an öffentlichen Orten soll die intelligente VÜ einen Beitrag zur Kriminalitätsprävention, Kriminalitätsrepression und zur Verbesserung des Sicherheitsgefühls in der Bevölkerung leisten. Mögliche Einsatzszenarien lassen sich daher viele konstruieren. Exemplarisch sollen vier mögliche Szenarien vorgestellt werden, bei denen das Potenzial der Analysemöglichkeit zum Tragen kommt und die intelligente VÜ dadurch eine Arbeitserleichterung und einen Mehrwert für die Sicherheitsbehörden entfaltet.

1. Multisensoriell gestützte Erfassung von Straftätern in Menschenmengen bei komplexen Einsatzlagen (Muskat)

Bei öffentlichen Veranstaltungen, wie Fußballspielen, kommt es regelmäßig zur Begehung von Straftaten in Form von z.B. Gewaltdelikten und Verstößen gegen das Sprengstoffgesetz oder durch das Zünden von Pyrotechniken. In der Fußballsaison 2015/2016 nutzen über drei Millionen Fußballfans das Reisemittel Bahn und dabei registrierte allein die Bundespolizei über 1.500 Straftaten.[98] Hier könnte das Muskat-System bei eskalierenden Gemengelagen bahnreisender Fußballfans zum Einsatz kommen. Bei solchen Einsatzszenarien findet bereits heute VÜ statt, doch diese wird manuell durch verschiedene Akteure (Bundes- und Landespolizei, DB AG etc.) durchgeführt. Im Nachgang müssen die Daten der unterschiedlichen Systeme, die oft nicht kompatibel sind, zusammengeführt und es muss aufwändig ermittelt werden, wer wann welche Aufnahme getätigt hat. Um eine tatverdächtige Person zu überführen und Beweise für eine Verurteilung zu sammeln, ist eine gute Aufnahmequalität und eine plausible Beweiskette unabdingbar.

Muskat ermöglicht den direkten Datenaustausch zwischen der am Einsatz beteiligten Bundes- und Landespolizei und stellt die Verknüpfung verschiedener Endgeräte miteinander her und speichert alle Daten auf einem (mobilen) Server.[99]

---

[98] Vgl. Bundespolizei Jahresbericht 2016, S. 71.
[99] Vgl. Geske: Technisch-ethisches Gutachten im Zuge des Projekts „Multisensoriell gestützte Erfassung von Straftätern in Menschenmengen bei komplexen Einsatzlagen“, S. 4.

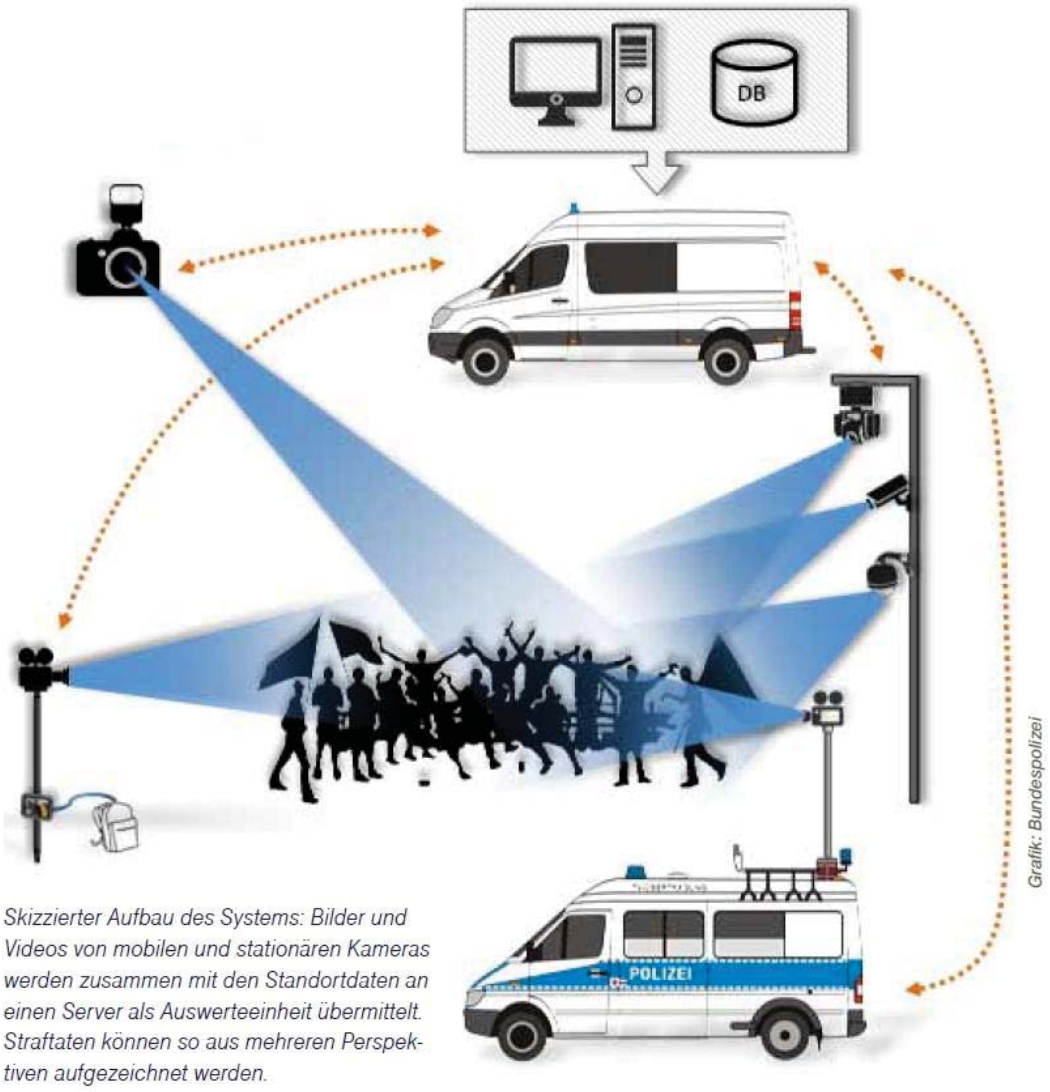


Abbildung 5: Skizzierter Aufbau von Muskat[100]

Gerade bei Fußballspielen kommt es immer wieder zur Begehung von Gewaltdelikten von Einzelpersonen aus einer Gruppe heraus. Aus einsatztaktischen Erwägungen wird die tatverdächtige Person nur selten direkt aus der Gruppe herausgeführt. Vielmals wird ein „günstiger Moment" gesucht, um die Person einer Identitätsfeststellung zu unterziehen. Hierfür ist entweder eine genaue Personenbeschreibung oder eine Video-/ Bildaufnahme der verdächtigen Person notwendig. Die Identifikation dieser Person anhand von gefertigten Video- und Bildmaterial stellt für die vor Ort eingesetzten Polizeikräfte eine enorme

[100] Bildquelle: Bundespolizei in Bundespolizei kompakt 03/2015: Muskat – Nicht nur ein Gewürz, S. 30.

Herausforderung dar. Auch die spätere Sichtung und Auswertung von Videomaterial für eine lückenlose Beweiskette, die eine tatverdächtige Person mit einer Straftat verbindet, ist mit einem hohen Aufwand verbunden. So dauert die Auswertung von einer Stunde Videomaterial ca. 10 Stunden und bindet dabei mehrere Ermittler.[101]

Bei der Identifizierung einer tatverdächtigen Person und bei der Auswertung des Videomaterials kann das Muskat-System behilflich sein. Durch den Einsatz eines Tracking-Algorithmus kann eine zuvor markierte Person Videogeräteübergreifend „verfolgt" werden. Dieses kann unter Nutzung softbiometrischer Beschreibungen, wie Kleidung, geschehen oder durch den Einsatz einer weiteren Software durch den Abgleich von Bilddaten des Gesichtes der tatverdächtigen Person.

Probleme bei der Auswertung von Videodateien stellt für die Ermittler oftmals der genaue Raumbezug von Tat und Tatverdächtigen sowie den weiteren Bewegungsablauf dar. Hier unterstützt Muskat durch die Darstellung der verschiedenen Kameraposition im Raum durch einen GPS-Sensor sowie die Kameraausrichtung (Position) durch einen IMU-Sensor. Dieser IMU-Sensor besteht aus einer räumliche Kombination mehrerer Inertialsensoren, wie Beschleunigungssensoren und Drehratensensoren.[102] Die Metadaten können in einer Übersichtskarte dargestellt werden. Dieses hat insbesondere bei Einsatzlagen mit wechselnden Örtlichkeiten und beim Einsatz mehrere Videokameras enorme Vorteile für eine lückenlose Beweiskette, da so die Kameras besser identifiziert werden können, die im Einsatz denselben Tatverdächtigen aus verschiedenen Perspektiven und Blickwinkeln videografiert haben.[103] Zusätzlich werden alle Videoaufnahmen mit einem Zeitstempel versehen, so dass anhand eines Zeitstrahls eine bessere Nachvollziehbarkeit beim nachträglichen Videoschnitt gewährleistet wird.

---

[101] Vgl. Geske: Technisch-ethisches Gutachten im Zuge des Projekts „Multisensoriell gestützte Erfassung von Straftätern in Menschenmengen bei komplexen Einsatzlagen", S. 12.
[102] Vgl. Hoffmann: Kombination von Inertialsensoren und GPS zur Navigation, S. 19.
[103] Vgl. Decker: Muskat – Nicht nur ein Gewürz in Bundespolizei kompakt, S. 29.

Das hier beschriebene technische Hilfsmittel der multisensoriell gestützten Erfassung von Straftätern in Menschenmengen soll helfen, tatverdächtige Personen im Videobild zu erkennen und zu verfolgen, um so die Aufklärung von Straftaten zu optimieren. Dadurch soll die quantitative und qualitative Beweissicherung bei Straftaten im Rahmen von öffentlichen Veranstaltungen erhöht werden. Durch die Entziehung „sicherer Räume", also die Möglichkeit für die Täter sich in großen Menschenansammlungen zu verstecken, soll eine Unsicherheit für die Begehung weiterer Straftaten hervorgerufen werden, so dass das System situationsbezogen kriminalpräventiven Charakter entfaltet. Zudem verkürzt das System die Videosichtungszeit und unterstützt die Videoanalyse im Anschluss an einen Vorfall durch die Bereitstellung von Metadaten und den optimierten Austausch von Daten durch die am Einsatz beteiligten Akteure.[104]

2. Analysesysteme zur Auswertung von Videomassendaten

Terroranschläge wie in Nizza, Paris oder Boston haben gezeigt, dass es für eine schnelle Aufklärung erforderlich ist, in relativ kurzer Zeit Video- und Bilddaten mit Tatortbezug auszuwerten.[105] An vielen Orten existieren bereits dutzende Videoüberwachungskameras, die durch (Polizei-) Behörden betrieben werden. Hinzu kommen noch unzählige weitere Kameras, die durch Private (Geschäfte, DB AG, Haushalte, etc.) betrieben werden. Bei Anschlagsszenarien und großen Schadensereignissen werden zudem noch hundertfach private Aufnahmen mit Kameras und Smartphones getätigt. Nach dem Sprengstoffanschlag auf den Boston-Marathon am 15. April 2013 bat die Polizei die Bevölkerung um Hilfe und die Zusendung von Fotos oder Videos, die unmittelbar vor und unmittelbar nach den Explosionen gemacht wurden, einzureichen. Innerhalb von 24 Stunden erhielten die Ermittler über 2.000 Hinweise aus der Bevölkerung.[106] Das Sammeln von Bild- und Videodaten aus der Bevölkerung wird nach diesem Ereignis mit den Begriffen „Boston-Cloud" oder „Boston-Infrastruktur" synonym verwandt. Auch in Deutschland wurden solche Hinweisportale zum Upload von Dateien anlassbezogen und für den Zeitraum

---

[104] Vgl. Geske: Technisch-ethisches Gutachten im Zuge des Projekts „Multisensoriell gestützte Erfassung von Straftätern in Menschenmengen bei komplexen Einsatzlagen", S. 18f.
[105] Vgl. BMBF: Projektbeschreibung FLORIDA, S. 1.
[106] Vgl. Zeit online: Überwachungskamera liefert Hinweis auf Attentäter vom 17.04.2013.

der Hinweisaufnahme bereitgestellt. Beispiele hierfür sind die Vorkommnisse zur Silvesternacht 2015/16 im Bereich des Doms in Köln. Insgesamt wurden über 1.100 Stunden Videomaterial gesichtet und ausgewertet. Videoquellen waren dabei insbesondere die Aufnahmen der DB AG vom Hauptbahnhof in Köln.[107] Hinzu kamen polizeiliche sowie private Videoaufzeichnungen aus der Bevölkerung in einem Umfang von über 700 Stunden.[108] Auch nach dem LKW-Anschlag auf den Berliner Weihnachtsmarkt an der Gedächtniskirche am 19. Dezember 2016 und den Ausschreitungen bei den Demonstrationen zum G20-Gipfel vom 07. und 08. Juli 2017 in Hamburg wurde eine Internet-Cloud geschaltet um Daten aus der Bevölkerung entgegenzunehmen. Allein hier sind nach Angaben der Soko Schwarzer Block über 7.000 Dateien hochgeladen worden, was einer zweistelligen Terabyte-Zahl an Daten entspricht. Hinzu kamen noch rund 25.000 „Einzelvideos“ von Polizisten und der Inhalt von mehr als 100 Festplatten aus Bussen, Bahnen und Bahnhöfen.[109] Den Ermittlungsbehörden mangelt es oftmals nicht an Videomaterial, um den Tathergang zu konstruieren und gegebenfalls Tatverdächtige zu ermitteln, sondern an den zeitlichen und personellen Ressourcen dies schnellstmöglich zu bewerkstelligen.

Diese Mengen an Daten stellen die Ermittlungsbehörden vor verschiedene Probleme. Die erste Hürde ist eine digitale Infrastruktur zu schaffen, die es ermöglicht große Datenmengen hochzuladen und zu speichern. Generell gelten Daten aus externen Quellen als „schmutzig“, da sie mit Viren bzw. Schadsoftware belasten sein können. Diese Daten müssen erst einmal strikt von den internen Servern der Ermittlungsbehörden getrennt werden, um eine Infiltrierung des Netzwerkes zu unterbinden. Für eine zielführende Auswertung der Daten müssen diese Videos dennoch mit denen der Polizei zusammengeführt werden.

---

[107] Vgl. Schulte: Die Silvesternacht 2015/16 in Köln - Darstellung der Ermittlungen der EG Neujahr (Teil 3), S. 14.
[108] Vgl. BMBF: Projektbeschreibung PERFORMANCE, S. 1.
[109] Vgl. Monroy: G20-Gipfel: Polizei durchsucht zehntausende Dateien mit Gesichtserkennungssoftware, S. 1.

Nachdem die Daten auf Schadsoftware geprüft wurden, gilt es, die verschiedenen Dateiformate der Videodateien kompatibel zu machen. Die originalen Videodateien werden auf einen externen Server archiviert. Im nächsten Schritt werden alle Sequenzen mit weiteren Daten annotiert. Hier werden Informationen angehängt bspw. über die zu sehenden Vorkommnisse, die Örtlichkeit und die Quelle der Daten. Dieses soll bei der späteren Ermittlung helfen, in den Massen der Dateien eine erste Vorsortierung vorzunehmen.

Erst dann beginnt die eigentliche Auswertung der Videodateien. Je nach Szenario unterscheiden sich die Zielsetzungen, die die Ermittler verfolgen. Bei einem terroristischen Selbstmordattentat geht es bspw. um die Rekonstruktion des Geschehensablaufs und die Ermittlung des Täters. Bei gewalttätigen Demonstrationen oder den Übergriffen bei der Silvesternacht in Köln geht es um die Zuordnung von Tätern zu Tathandlungen. Videoanalyseprojekte, wie FLORIDA, versuchen neue Verfahren zur zeitlich-räumlichen Referenzierung der vorhandenen Videos zu entwickeln, um so Möglichkeiten zu schaffen, eine dreidimensionale Rekonstruktion der Szene, sowie die automatische Detektion von frei zu definierenden Objekten untersuchen zu können.[110]

Für eine optimale Rekonstruktion eines Geschehensablaufs und der daraus sich verfestigenden Beweiskette für spätere Gerichtsverfahren ist es notwendig, unterschiedliche Perspektiven der Tathandlungen auszuwerten. Schwierigkeiten können sich durch Tathandlungen ergeben, die nicht auf einen Tatort beschränkt sind, wie zum G20-Gipfel in Hamburg, als der „Schwarze Block“ durch die Innenstadt zog und immer wieder durch Straftaten, wie Landfriedensbruch, Körperverletzungsdelikte und „Plünderungen“ aufgefallen ist.[111] Um einer Person alle begangenen Tathandlungen zuordnen zu können, müssen hunderte Stunden Videomaterial ausgewertet werden. Auch hier kann eine Analysesoftware als Werkzeug für die Ermittler dienen. FLORIDA verfolgt den Ansatz zur Interoperabilität. So können Ermittler über graphische Anwendungen in der Lage sein, Ergebnisse, die durch die Vorverarbeitung der Video-

[110] Vgl. BMBF: Projektbeschreibung FLORIDA, S. 1.
[111] Vgl. Kipp: „Alles normal“ – Nach G20-Krawallen wieder Alltag im Schanzenviertel, S. 1.

massendaten auf der Plattform generiert wurden, zu nutzen und in die Ermittlungen einzubeziehen.[112] Dies ermöglicht ein paralleles Arbeiten mehrerer Ermittler an einem Vorgang, ohne dabei aneinander vorbei zu ermitteln. Das Projekt der kooperativen Systemplattform für Videoupload, Bewertung, teilautomatisierte Analyse und Archivierung geht noch einen Schritt weiter und prüft die rechtlichen sowie sozialen Rahmenbedingungen zur Schaffung von Schnittstellen zur Einbindung privater Dienstleister in die Erhebung und Auswertung der Videodaten, zur Überbrückung von Engpässen in großen Ermittlungsverfahren und Anschlagsszenarien.[113]

Zur Unterstützung bei der Archivierung von Videodateien und der Rekonstruktion von Geschehensabläufen können die Videomassendaten auch nach Inhalten durchsucht werden. Neben angelegten Örtlichkeiten kann auch eine Personensuche mit Filtern eingesetzt werden. Hierbei können softbiometrische Beschreibungen, wie Kleidung oder spezieller Kennzeichen auch „etwa das Alter, Geschlecht oder die ethnische Zugehörigkeit eingegrenzt werden“.[114] Aber auch die Nutzung von biometrischer Gesichtserkennung zum Verfolgen einer Person ist nicht ausgeschlossen. Ist das biometrische Template einer Person angelegt, so ist es für ein leistungsfähiges Videomanagementsystem möglich, die Person „wiederzuerkennen“ und alle Videodaten mit dieser Person anzuzeigen.[115] In einem weiteren Schritt könnten erkannte Gesichter mit (Fahndungs-)Datenbeständen abgeglichen werden.[116]

Durch Analysesysteme zur Auswertung von Videomassendaten werden Tathergänge schneller rekonstruiert und potentielle Tatverdächtige zeitnah ermittelt und dadurch den Aufwand für Personal und Zeit bei den Ermittlungsbehörden erheblich reduziert.[117]

---

[112] Vgl. BMVIT: Produktbeschreibung FLORIDA
[113] Vgl. Eigenseer/Humer/Lederer: Von der konventionellen zur intelligenten Videoüberwachung in Digitale Polizeiarbeit, S. 153; BMBF: Projektbeschreibung PERFORMANCE, S. 1.
[114] Vgl. Monroy: G20-Gipfel: Polizei durchsucht zehntausende Dateien mit Gesichtserkennungssoftware, S. 1.
[115] Vgl. Videmo Intelligente Videoanalyse: Produktbeschreibung Videmo 360
[116] Vgl. Monroy: G20-Gipfel, S. 1.
[117] Vgl. BMBF: Projektbeschreibung FLORIDA, S. 1.

3. Identitätsfeststellung

Die Feststellung der Identität (Personalien) von Personen an einem Tatort ist eine der häufigsten polizeilichen Maßnahmen im Ersten Angriff. Rechtlich unterscheidet man zwischen der Identitätsfeststellung zur Gefahrenabwehr nach Polizeirecht und der strafprozessualen IDF.[118] Das geschieht im Regelfall durch den Abgleich der Person und einem Dokument (BPA, Reisepass), welches die Identität legitimiert. Eine weitere Möglichkeit, die Identität einer Person festzustellen, ist die erkennungsdienstliche Behandlung. Hierunter versteht man die Erfassung und den Abgleich von personenbezogenen und biometrischen Daten (bspw. Bilder, Daktylogramm) einer Person durch die Polizei.[119]

Eine Gesichtserkennungssoftware kann im Fall einer auf Video aufgenommenen Straftat das Gesicht des mutmaßlichen Täters mit polizeilichen Datenbeständen (bspw. INPOL) abgleichen und so die Identität des Gesuchten ermitteln. Bereits heute versucht man, Personen, die bei einer Straftat gefilmt wurden durch den manuellen Abgleich von Bilddatenbanken zu identifizieren. Je nach Schwere der Straftat und der Erfüllung der rechtlichen Voraussetzungen kann das unter zur Hilfenahme der Bevölkerung, durch Öffentlichkeitsfahndung gem. § 131b StPO geschehen. Dieses Verfahren ist jedoch sehr zeit- und personalintensiv und mit schwerwiegenden Eingriffen in die Rechte des Betroffenen verbunden. Heutige Software verspricht in diesem Verfahren Unterstützung. So lassen sich große Bild- oder Videodatenbanken halbautomatisch, das heißt durch eine automatische Entscheidung in all den Fällen, in denen sich der Algorithmus sehr sicher ist, abgleichen und nur bei Bildern mit einer geringen Wahrscheinlichkeit der Übereinstimmung werden die Treffer noch einem Menschen zur Entscheidung vorgelegt. Dies bedeutet eine erhebliche Arbeitszeitersparnis und Steigerung der Treffergenauigkeit, da ein Algorithmus rund um die Uhr und mit gleichbleibender Leistung arbeitet.[120]

---

[118] Vgl. Ackermann/Clages/Roll: Handbuch der Kriminalistik, S. 41.
[119] Vgl. Creifelds: Rechtswörterbuch, Erkennungsdienstliche Maßnahme, S. 379.
[120] Vgl. Videmo Intelligente Videoanalyse: Produktbeschreibung FaceSDK.

4. Personenfahndung

Das vierte Einsatzszenario für eine iVÜ kann die Personenfahndung sein. Die Polizeidienstvorschriften definieren polizeiliche Fahndung mit: „alle Maßnahmen und Einrichtungen zur planmäßigen Suche nach Personen und Sachen im Rahmen der Strafverfolgung und zum Schutz der öffentlichen Sicherheit und Ordnung."[121] Die Fahndung ist ein wichtiges Tätigkeitsfeld der polizeilichen Gefahrenabwehr und der Verbrechensbekämpfung.[122]

Anders als bei den ersten drei Szenarien kommt hier die Analyse- und Auswertefunktion nicht bei einem konkreten Ereignis (Straftat) zum Tragen, sondern wäre ubiquitär. Eines konkreten Anlasses bedürfte es indes nicht. Die Grenzen der Einsatzmöglichkeiten wären durch die gesetzlichen Vorgaben analog der konventionellen VÜ des öffentlichen Raums in den entsprechenden Polizeigesetzen zu sehen. Technisch wäre es möglich, alle im öffentlichen Raum befindlichen Videokameras, die durch die Polizeien betrieben werden, mit einer Software auszustatten, die es erlaubt, alle gefilmten Gesichter mit einem Gesichtserkennungsprogramm auszulesen. Die so erstellten Templates könnten dann mit einer Fahndungsdatenbank verknüpft und mit den in der Datenbank abgelegten Gesichtern gesuchter Personen abgeglichen werden. Im Falle eines Treffers würde dann eine Treffermeldung ausgeworfen werden, die es den Behörden ermöglicht, weitere Maßnahmen zu treffen.[123]

Im Rahmen des gemeinsamen Pilotprojekts "Sicherheitsbahnhof Berlin Südkreuz" testet die Bundespolizei Systeme zur automatisierten Gesichtserkennung.[124] Ziel dieses Projektes ist es, einen zuvor in einem System eingepflegten Personenkreis aus der Menge der vielen täglichen Nutzer des Bahnhofes herauszufiltern und die Trefferwahrscheinlichkeit zu ermitteln. Für diesen Versuch wurde nur ein kleiner Testbereich im Bahnhof Südkreuz deklariert. Sollte der Versuch erfolgreich sein und ausgeweitet werden, so stünde allein der Bundespolizei ein Netz von derzeit über 6.000 Videokameras auf ca. 900 Bahnhöfen zur Verfügung. Derzeit sind nicht alle Kameras geeignet, um mit

---

[121] PDV 384.1 in Ackermann/Clages/Roll: Handbuch der Kriminalistik, S. 249.
[122] Vgl. Ackermann/Clages/Roll: Handbuch der Kriminalistik, S. 249.
[123] Vgl. Hornung/Schindler: Das biometrische Auge der Polizei, S. 207.
[124] Vgl. BMI: Pressemitteilung – „Sicherheitsbahnhof Berlin Südkreuz", S. 1.

einer Videoanalysesoftware ausgestattet zu werden. Die DB AG baut jedoch ihr Netz an Videoüberwachungsanlagen kontinuierlich aus.[125]

III Zusammenfassung

Mögliche Einsatzfelder einer iVÜ, wie das Erkennen und Verfolgen von Personen anhand einer Gesichtserkennung in Live-Bildern und gespeicherten Videodateien, sind denkbare Szenarien zur technischen Unterstützung der Strafverfolgungsbehörden. Darüber hinaus lassen sich noch weitere Einsatzmöglichkeiten intelligenter Systeme konstruieren. Ob sich diese in der Praxis als tauglich erweisen und nicht nur leere Versprechen der Softwareentwickler sind, müssen weitere Real-Tests, wie derzeit am „Sicherheitsbahnhof Berlin Südkreuz“ und unabhängige Evaluationsstudien zeigen. Nicht jede technische Errungenschaft, die mehr Sicherheit propagiert, ist per se legitimiert und akzeptiert, sondern ist vielmehr an hohe juristische und gesellschaftliche Hürden gebunden.

Die Erwartungen in die Technik der VÜ auf Seiten der Politik sind hoch. So wird vielmals als Reaktion auf Kriminalität und Terrorismus der Ausbau der VÜ diskutiert[126] und der Forderung mit neuen Gesetzen, wie dem Videoüberwachungsverbesserungsgesetz, Rechnung getragen.[127] Ob eine iVÜ tatsächlich ein geeignetes Mittel zur Kriminalitätsvorsorge und -bekämpfung und nicht nur eine Arbeitserleichterung der Polizeibehörden ist, wird nachfolgend anhand der Wirksamkeit „intelligenter“ Videoüberwachung im Vergleich zur konventionellen VÜ untersucht.

---

[125] Vgl. BMI: Pressemitteilung – „Sicherheitsbahnhof Berlin Südkreuz, S. 2.
[126] Vgl. Hornung/Schindler: Das biometrische Auge der Polizei, S. 203.
[127] Vgl. BGBl I 2017 Nr. 23, S. 968 ff.

E Wirksamkeit „intelligenter“ VÜ im Vergleich zur konventionellen VÜ

„Für Ihre Sicherheit wird dieser Bereich videoüberwacht“ – So oder so ähnlich sind Hinweisschilder gekennzeichnet, die den Bürger darauf aufmerksam machen sollen, dass an diesem Ort VÜ stattfindet. Mit Hinweisschildern werden die Polizeibehörden den rechtlichen Vorgaben gerecht, die einen offen Einsatz von Videokameras zum Beobachten und Aufzeichnen nur erlauben, wenn „der Umstand der Überwachung und die verantwortliche Stelle [...] durch geeignete Maßnahmen erkennbar“[128] sind.

Dieser Satz impliziert, dass polizeiliche VÜ des öffentlichen Raumes nicht als Arbeitserleichterung der Polizeibehörden zu verstehen ist, sondern wesentliche Ziele verfolgt, den Bürger zu schützen. VÜ hat im Wesentlichen drei primäre Ziele. Die Verhinderung von Straftaten, die Aufklärung von bereits eingetretenen Rechtsgutsverletzungen und die daraus resultierende Stärkung des Sicherheitsgefühls in der Bevölkerung.[129] Um die Wirksamkeit von VÜ bewerten zu können, muss man sich mit dem Begriff Sicherheit auseinandersetzen. Sicherheit stellt einen gesellschaftlichen Zentralwert dar und bezieht sich dabei auf unterschiedlichste Bereiche. Neben der Vermeidung von Kriminalität, Kriegen und Gewalt gehören auch soziale Faktoren, wie Armut, zu den zentralen Punkten. Für Sicherheit zu sorgen, ist eine grundlegende Aufgabe des Staates. „Aus dem Schutz seiner Bürger legitimiert der Staat seine Existenz, die Pflichten seiner Bürger und zugleich die Einschränkung ihrer Rechte, letztlich also seinen Herrschaftsanspruch.“[130]

Die Kompetenz des Staates, Sicherheit zu gewährleisten, beruht dabei nicht nur auf der Fähigkeit, angemessen auf Rechtsgutverletzungen zu reagieren, sondern vielmehr, ob es ihm gelingt, erfolgreich präventiv tätig zu werden und dabei Unsicherheit und Ordnungsverstöße zu verhindern, bevor sie eintreten.[131] Dies kann mit unterschiedlichsten Mitteln geschehen, bspw. durch den Einsatz technischer Hilfsmittel, wie der polizeilichen VÜ. Doch Kameras alleine

---

[128] Exemplarisch: § 14 Abs. 3 S. 2 HSOG.
[129] Hornung/Desoi: "Smart Cameras" und automatische Verhaltensanalyse, S. 153.
[130] Apelt/Möllers: Wie „intelligente“ Videoüberwachung erforschen?, S. 586.
[131] Vgl. Glaeßner: Sicherheit und Freiheit, S. 11.

können noch keine Straftaten verhindern, jedoch kann die Präsenz potenzielle Täter davon abschrecken, Straftaten zu begehen. „Überdies können Videoaufzeichnungen im Rahmen der Strafverfolgung zur Gewinnung von Ermittlungsansätzen, zur Identifizierung von Straftätern sowie als Beweismittel vor Gericht herangezogen werden“[132] *Apelt/Möllers* und *Zurawski* definieren darüber hinaus zwei weitere Ziele der VÜ. Die Reduzierung von Kosten für die Überwachung von Objekten und Räumen durch Personaleinsparungen[133] und die Disziplinierung der Verhaltensweisen der Nutzer der beobachteten Räume.[134]

Während es zur Effizienz der konventionellen VÜ verschiedene Studien gibt, lässt sich dies für eine iVÜ aufgrund des unzureichenden praktischen Einsatzes nicht bestätigen. Der polizeiliche Einsatz von VÜ ist eine umstrittene Maßnahme, nicht nur weil sich ihr Mehrwert schwer oder gar nicht messen lässt. Je nachdem, welche Bewertungskriterien man heranzieht, um die Effektivität von VÜ festzustellen, desto unterschiedlicher werden die Ergebnisse ausfallen. Ausgehend vom derzeitigen Ist-Zustand werden die fünf Ziele der VÜ auf ihre Effizienz näher betrachtet und soweit wie möglich eine Ableitung zum Einsatz intelligenter Systeme vorgenommen.

I VÜ als Werkzeug der Kriminalprävention

„Freiheit braucht Sicherheit und Sicherheit braucht Prävention. Dieser Programmsatz ist in Staat und Gesellschaft, besonders aber in der kriminalpolitischen Debatte allgegenwärtig und unangefochten.“[135] Oftmals wird diese Forderung mit dem Ausbau von VÜ gleichgestellt, denn diese gilt als „sicherheitspolitische Wunderwaffe“.[136] Ihr Ruf ist vielmals besser, als die tatsächliche Effektivität im Rahmen der Gefahrenabwehr und dennoch wird ihr Einsatz hartnäckig verteidigt und die Technik im Zweifel ausgebaut.[137]

---

[132] Hornung/Schindler: Das biometrische Auge der Polizei, S. 203.
[133] Vgl. Apelt/Möllers: Wie „intelligente“ Videoüberwachung erforschen?, S. 589.
[134] Vgl. Zurawski: Raum-Weltbild -Kontrolle, S. 153.
[135] Zabel: Das Paradox der Prävention in Der Staat und die Sicherheitsgesellschaft, S. 56.
[136] Schnabel: Die polizeiliche Videoüberwachung öffentlicher Orte in Niedersachen, S. 879.
[137] Vgl. ebd., S. 880.

1. Konventionelle VÜ als Instrument der Kriminalitätsbekämpfung

In Deutschland gibt es bisher nur wenige Studien, die die tatsächliche Effizienz der öffentlichen VÜ als Instrument der Kriminalitätsbekämpfung differenziert und umfänglich untersuchen.[138] Es wurde in den letzten Jahren mehrfach versucht, die Wirksamkeit staatlicher präventiver VÜ durch Untersuchungen und Studien zu messen, jedoch wiesen viele dieser Studien umfassende Mängel an empirischen Datenmaterial auf und „zeichnen ein ambivalentes Bild der Wirksamkeit der Videoüberwachung."[139] Dieses reicht von Vertretern, die in der VÜ eine grundsätzliche kriminalpräventive Wirkung erkennen, über differenzierte Ansichten, die diese Wirkung nur für gewisse Delikte bzw. Örtlichkeiten sehen und Vertretern, die der staatlichen VÜ sehr kritisch gegenüber stehen oder der VÜ eine kriminalpräventive Wirkung gänzlich absprechen.[140]

a) Rational Choice Ansatz

VÜ hat zum Ziel, den potenziellen Täter durch Erhöhung des Entdeckungsrisikos von der Tat abzuhalten.[141] Diesem Denkansatz liegt zugrunde, dass sich der Täter aufgrund einer Kosten-Nutzen-Analyse dazu entscheidet, eine Straftat zu begehen oder es zu unterlassen. Diese Theorie des rationalen Wahlhandelns (rational choice approach), auch als ökonomische Kriminalitätstheorie bezeichnet, ist ein Ansatz der Handlungstheorie, die die Handlungen von Individuen, sowie deren Folgen darlegt. Die Grundprinzipien, nach denen sich das menschliche Handeln richtet, sind Nutzenmaximierung und Kostenminimierung.[142] Nach dieser Theorie ist Kriminalität das Ergebnis freier und rationaler Wahlentscheidungen der Menschen in unterschiedlich abzuwägenden Situationen. Infolgedessen schätzt das Individuum den subjektiven Nutzen der Tat (Wert der Beute), sowie die subjektiven Kosten der Tat, wie etwa die Wahrscheinlichkeit der Entdeckung, der Aufklärung der Tat und die sich daraus ergebenden strafrechtlichen Sanktionen sowie die möglichen gesellschaftlichen Folgen ein. Diesem Ansatz folgend werden Straftaten unwahrscheinlicher, wenn „erstens angedrohte Strafen dem kriminellen Handeln mit Sicherheit und

---

[138] Vgl. BT-Drucksache 17/13071, S. 1.
[139] Starnecker: Videoüberwachung zur Risikovorsorge, S. 26.
[140] Vgl. ebd., S. 26.
[141] Vgl. Maximini: Polizeiliche Videoüberwachung, S. 14.
[142] Vgl. Schwind: Kriminologie, § 6, S. 125.

zweitens in geringer zeitlicher Verzögerung folgen und so schwer sind, dass drittens ihre Kosten den durch die kriminelle Handlung zu erzielenden Nutzen überwiegen."[143]

Ein rational denkender Mensch würde nach der Abwägung von Kosten und Nutzen seiner Tat zu dem Entschluss kommen, dass sich die Begehung einer Straftat in einem Bereich, der durch die Polizei videoüberwacht wird, nicht lohnt („Crime doesn`t pay").[144] Die Tathandlung könnte in Echtzeit über Kameras durch Polizeibeamte beobachtet werden, alternativ aufgezeichnet und so eine Überführung des Täters im Nachgang möglich werden.

Die VÜ muss als offene Maßnahme durchgeführt werden, damit der potenzielle Täter das Entdeckungsrisiko in seiner Kosten-Nutzen-Rechnung einfließen lassen kann.[145] Eine dauerhafte präventive Wirkung dieser Abschreckungsthese hat nur Bestand, wenn der Täter weiß, dass er gerade aufgrund der VÜ eher der Tat überführt und dadurch mit einer Bestrafung zu rechnen hat. „Deshalb muss, für die Bevölkerung nachvollziehbar, die Aufklärungsquote als Folge der Überwachung gesteigert und das Risiko für den Täter größer werden."[146] Einige Länderpolizeibehörden arbeiten transparent mit den Erfahrungen/ Ergebnissen aus der polizeilichen VÜ. Das Hessische Landeskriminalamt gab für den Zeitraum der letzten fünf Jahre an, dass es „im Zusammenhang mit der Beobachtung der Videomonitore aufgrund von notwendigen Sofortinterventionen zu 1.750 gefahrenabwehrenden Maßnahmen (Platzverweise, Durchsuchungen von Personen und Sachen, Sicherstellungen, Ingewahrsamnahmen) kam."[147]

Ob ein potenzieller Täter Kenntnis von diesen (Erfolgs-) Zahlen hat und zu welcher Schlussfolgerung man in Bezug auf die Effektivität der VÜ kommen kann, ist nicht nachweisbar. Eindringlicher dürften Öffentlichkeitsfahndungen gem. § 131b StPO aufgrund durch Videokameras gefertigte Tatbilder sowie

---

[143] Eifler/Brandt: Videoüberwachung in Deutschland, S. 157f.
[144] Ebd., S. 158.
[145] Vgl. Glatzner: Die staatliche Videoüberwachung des öffentlichen Raumes, S. 17.
[146] Maximini: Polizeiliche Videoüberwachung, S. 14.
[147] HLKA: Handlungsempfehlung für die Errichtung und den Betrieb von Videoüberwachungsanlagen im öffentlichen Raum, S. 7.

Erfolgsmeldungen der Polizei, wie bspw. „Polizei sucht mit Foto nach U-Bahn-Schläger - Der Tatverdächtige konnte ermittelt werden“[148], sein. Damit sich der Täter diesem erhöhten Sanktionsrisiko ausgesetzt sieht, muss er dafür intellektuell in der Lage sein, die Vor- und Nachteile seines Handelns gegenseitig abzuwägen.[149] Zudem wird gegen diesen Ansatz eingewandt, dass viele Delikte spontan und affektiv begangen werden und eben nicht nach einer rationellen Kosten-Nutzen-Rechnung. „Demnach kann angenommen werden, dass die Videoüberwachung für die Verhinderung von Affekt-, Spontan-, Rausch- oder Beziehungstaten kein geeignetes Mittel darstellt.“[150]

Der Ausbau der VÜ wird auch gerne im Kampf gegen terroristische Anschläge propagiert.[151] Doch gerade bei solchen Szenarien ist die präventive Wirkung von VÜ fraglich, insbesondere, wenn es sich bei einem Anschlag durch einen Selbstmordattentäter handelt. Gerade ihm ist es egal, ob er bei der Tat gefilmt wird oder nicht, zum Teil gehört es sogar zur Inszenierung des Attentats. Die Abschreckungswirkung von Videokameras hängt immer von der persönlichen Risikobereitschaft des Täters und der Furcht vor den Konsequenzen seiner Entdeckung ab und kann folgerichtig nicht für alle Tätergruppen gleichermaßen geeignet sein.[152] VÜ kann also bei bestimmten Deliktsarten, an bestimmten Orten und bei bestimmten Tätertypen eine kriminalpräventive Wirkung durch Abschreckung hervorrufen. Dies belegen unterschiedliche nationale und internationale Studien. Im statistischen Durchschnitt ließ sich nur eine Senkung der Kriminalität von 4% nachweisen.[153] Andere Studien konnten hinge-

---

[148] Berliner Morgenpost: Polizei sucht mit Foto nach U-Bahn-Schläger vom 01.11.2017, auf https://www.morgenpost.de/berlin/polizeibericht/article212407833/Polizei-sucht-mit-Foto-nach-U-Bahn-Schlaeger.html, abgerufen am 23.11.2017.
[149] Vgl. Maximini: Polizeiliche Videoüberwachung, S. 14.
[150] Glatzner: Die staatliche Videoüberwachung des öffentlichen Raumes, S. 17f.
[151] Vgl. Hegemann/Kahl: Terrorismus und Terrorismusbekämpfung, S. 164; vgl. BT-Drucksache 18/10941, S. 2.
[152] Vgl. Glatzner: Die staatliche Videoüberwachung des öffentlichen Raumes, S. 18.
[153] Vgl. Bücking: Polizeiliche Videoüberwachung öffentlicher Räume, S. 47; vgl. Bücking/ Kubera: „Eine digitale Streifenfahrt…“, S. 316f.; vgl. Welsh/ Farrington: Crime prevention effects of closed circuit telvision, S. 42; vgl. Glatzner: Die staatliche Videoüberwachung des öffentlichen Raumes, S. 60.

gen einen Rückgang der Gesamtkriminalität in einem videoüberwachten Bereich von über 50% nachweisen.[154] Aber auch bei rational entscheidenden Tätertypen lässt sich die abschreckende Wirkung der VÜ nur solange aufrechterhalten, solange dem Täter Konsequenzen aus seiner Tathandlung drohen. Aufgrund der Vielzahl der im öffentlichen Raum zu findenden Videokameras kann ein rational agierender Täter auch zu dem Entschluss kommen, dass es den Polizeibehörden gar nicht möglich ist, alle Videobilder auszuwerten und schon gar nicht in Echtzeit zu sichten.

Der Rational Choice Ansatz ist aber nur eine von verschiedenen Kriminalitätstheorien die versuchen zu erklären, warum es zur Begehung von Straftaten kommt[155] und ob eine Beeinflussung der Täterhandlung durch externe Faktoren, wie Videoüberwachungsmaßnahmen, soweit möglich ist, dass eine Tat nicht begangen wird.

b) Routine Activity Approach

Ein anderer Ansatz ist der Routine Activity Approach von *Cohen* und *Felson*[156]. Dieser weist Parallelen zu dem Rational Choice Ansatz auf, da beide Konzepte davon ausgehen, dass Kriminalität von den Gelegenheiten abhängig ist. Bei dem Routine Activity Approach wird versucht, die Kriminalitätsrate mit „den alltäglichen Mustern der Lebensführung bestimmter Bevölkerungskreise in Verbindung“[157] zu setzen. Unter diesen alltäglichen Mustern werden Routineaktivitäten (Routine Activity) als Dinge des täglichen Lebens, wie Arbeit oder Freizeitaktivitäten, verstanden. Nach *Cohen* und *Felson* werden drei Gegebenheiten herausgestellt, die die Gefahr einer Viktimisierung erhöhen:

Das Vorhandensein eines motivierten Täters (motivated offender), der auf ein geeignetes Opfer bzw. Tatobjekt (availability of a suitable target) trifft, dass nicht hinreichend geschützt ist (absence of capable guardians against a violation).[158]

---

[154] Vgl. Knape: Videogeräteeinsatz, S. 207.
[155] Vgl. Herrmann: Kriminalitätstheorien, auf http://www.krimlex.de/artikel.php?BUCHSTABE=K&KL_ID=108, abgerufen am 24.11.2017.
[156] Vgl. Cohen/Felson: Social Change and Crime Rate Trends, S. 588f.
[157] Glatzner: Die staatliche Videoüberwachung des öffentlichen Raumes, S. 18.
[158] Vgl. Cohen/Felson: Social Change and Crime Rate Trends, S. 589.

Abbildung 6: Darstellung des Routine Activity Approach

Dieser Schutz kann aus Personen („Wächtern") oder Umständen (Videoüberwachung) bestehen. Für *Cohen* und *Felson* ist das Zusammentreffen dieser drei Faktoren in räumlicher und zeitlicher Hinsicht entscheidend, da sie versuchen die „Routineaktivitäten" zu analysieren, die zu solch einem Zusammentreffen führen, um dadurch die Wahrscheinlichkeit krimineller Ereignisse zu bestimmen.[159] Um Straftaten zu verhindern, muss das Zusammentreffen der drei Faktoren unterbunden werden. Wie auch beim Rational Choice Ansatz geht das durch die Veränderung der Gelegenheitsstruktur, um so den Aufwand für den Täter bzw. die Kosten für die Straftat zu erhöhen.[160]

Die Etablierung von Videokameras kann dazu führen, dass ein Zusammentreffen der drei Faktoren unterbunden wird, da der Täter erschwerte Tatgelegenheiten vorfindet. Diese Annahme hat nur solange Bestand, wie der Täter annehmen muss, dass die Videobilder auch ausgewertet werden.

[159] Vgl. Glatzner: Die staatliche Videoüberwachung des öffentlichen Raumes, S. 18.
[160] Vgl. Schwind: Kriminologie, § 8, S. 160.

c) Fazit

Beide Ansätze sind der situativen Kriminalprävention zuzuordnen, da sie auf eine Veränderung der Umgebung abzielen. Dadurch soll das deliktische Verhalten erschwert und die Tat für den Täter risikoreicher und weniger lukrativ werden.[161] Beide genannten Ansätze geben verschiedene Anknüpfungspunkte für die kriminalpräventive Wirkung von VÜ. Während der Rational Choice Ansatz davon ausgeht, dass „durch die Installierung von Kameras an öffentlichen Plätzen das Entscheidungskalkül des Täters beeinflusst“[162] wird und dadurch das abweichende Verhalten für ihn unprofitabel erscheint, so kann nach der Annahme des Routine Activity Approach eine Straftat dadurch verhindert werden, dass eine der drei genannten Bedingungen für die Begehung von delinquenten Handlungen fehlt oder gehemmt ist. VÜ kann hier auf alle drei Faktoren Einfluss nehmen. Polizeiliche VÜ kann dem potenziellen Täter die Motivation nehmen, eine Straftat zu begehen, da er sich einem Entdeckungsrisiko ausgesetzt sieht. Durch die bewusste Wahrnehmung von Videokameras kann bei den potenziellen Opfern ein risikobewussteres Verhalten eintreten, so dass sie kein geeignetes Zielobjekt/ Opfer mehr darstellen. Zudem entspricht VÜ dem Konzept des Wächters (guardian). Kameras können so als technischer Surrogat angesehen werden.[163]

Videokameras können demnach ein probates Mittel darstellen, um Einfluss auf potenzielle Täter und Tathandlungen zu nehmen. Jedoch ist „die Auswirkung der Videoüberwachung in Bezug auf Täter und Delikte sehr differenziert“[164] zu betrachten. Es liegt die Vermutung nahe, dass nicht in jedem räumlichen Kontext und bei jedem Täter(-typ) dieselben Mechanismen greifen. Die präventive Wirkung muss auf unterschiedliche Weise hergestellt oder kompensiert werden. Wie andere Kriminalitätsbekämpfungsmaßnahmen muss auch die polizeiliche VÜ an die spezifischen Gegebenheiten vor Ort angepasst werden und

---

[161] Vgl. Tillich: Polizeiliche Videobeobachtung öffentlich zugänglicher Straßen und Plätze in München und Barcelona, S. 28.
[162] Ebd. S. 35.
[163] Vgl. ebd., S. 34.
[164] Glatzner: Die staatliche Videoüberwachung des öffentlichen Raumes, S. 18.

veränderten Rahmenbedingungen, wie bspw. Anpassungsstrategien der Täter oder Gewöhnungseffekte in der Bevölkerung, flexibel begegnet werden.[165]

Insbesondere bei terroristischen Anschlägen ist durch die VÜ keine abschreckende Wirkung festzustellen. Damit VÜ überhaupt abschreckend auf den potenziellen Täter wirkt, muss er von der Wirksamkeit dieser technischen Maßnahme überzeugt sein. So können schon die mediale Diskussion über den Ausbau von polizeilicher VÜ an einem bestimmten Ort (sogenannter „Placebo-Effekt“) oder Kameraattrappen zur Reduzierung der Gesamtkriminalität führen.[166] Die präventive Wirkung kann aber nach einiger Zeit nachlassen, wenn bspw. das Risiko einer Sanktion trotz VÜ für den Täter nicht ansteigt. [167] Der Täter muss im Glauben sein, dass seine Tat beobachtet bzw. aufgezeichnet wird, um ihn dann dieser zu überführen. Dieser Glaube kann durch eine schnelle Interaktion von Polizisten erzeugt und durch den Erfolg von weiteren Maßnahmen, wie (Öffentlichkeits-) Fahndungen aufrechterhalten werden.

Bei der hohen Anzahl von Videokameras im öffentlichen Raum ist eine Live-Auswertung nur in wenigen Fällen möglich. Allein im Zuständigkeitsbereich der Bundespolizei werden etwa 50 von 900 Bahnhöfen in Echtzeit überwacht und ausgewertet, was aber bei über 6.000 Videokameras nur einen Bruchteil darstellt.[168] Eine unmittelbare Interaktion aufgrund eines über Videomonitor beobachteten strafrechtlichen Sachverhalts stellt daher eher die Ausnahme als die Regel dar. Umso wichtiger ist es, polizeiliche Ermittlungserfolge, die auf Grundlage von gefertigten Videomaterials zustande gekommen sind, medial zu verbreiten, um so die Effektivität von Videoüberwachung aufrecht zu erhalten und einen Gewöhnungseffekt zu vermeiden.

Neben einer kriminalpräventiven Wirkung auf Seite des potenziellen Täters werden der VÜ weitere Wirkungsweisen zugeschrieben, die einen angestrebten Kriminalitätsrückgang begründen. *Armitage, Smyth* und *Pease* fassen diese wie folgt zusammen:

---

[165] Vgl. Dietrich: Wirksamkeit der polizeilichen Videoüberwachung, S. 13.
[166] Bücking/ Kubera: „Eine digitale Streifenfahrt…“, S. 317.
[167] Vgl. Lingg: Videoüberwachung im öffentlichen Raum, S.45.
[168] Vgl. BMI: Pressemitteilung – „Sicherheitsbahnhof Berlin Südkreuz“, S. 1.

„Effective Deployment“:	Durch die VÜ kann Sicherheitspersonal direkt zu verdächtigen Situationen geleitet werden, um unmittelbar bevorstehende Straftaten zu verhindern.
„Caught in the act“:	Täter werden durch die VÜ ermittelt und ggf. festgenommen und können daher keine weiteren Taten begehen.
„You've been framed“:	Abschreckung potentieller Täter durch ein erhöhtes Entdeckungsrisiko.
„Time for Crime“:	Verhinderung von Straftaten mit einem erhöhten Zeitbedarf oder die mit besonderen Anstrengungen verbunden sind, da durch eine VÜ für eine mögliche Straftat bis zu ihrer Entdeckung reduziert wird.
„Nosy parker“:	Kameraüberwachte Orte können das subjektive Sicherheitsgefühl der Bevölkerung stärken und ehemalige Angstorte werden wieder stärker frequentiert, wodurch potentielle Täter abgeschreckt werden könnten.
„Publicity“:	Eine mediale Berichterstattung zum Thema VÜ wird von den Bürgern als Indiz aufgefasst, dass die Kriminalität von staatlicher Seite aus ernst genommen wird. Dies kann Bürger zu gesetzeskonformem Verhalten ermutigen.
„Memory jogging“:	Die Anwesenheit von Kameras und Hinweisschildern kann für die Bürger ein Indiz sein, dass es sich um einen „gefährlichen Ort“ handelt und sie dadurch ermutigt werden eigene Sicherheitsvorkehrungen zu treffen. Dadurch werden weitere Tatgelegenheiten reduziert.
„Anticipated shaming“:	Straftaten unterbleiben, da man nicht als Täter bekannt werden möchte. Die VÜ dient als Mittel der sozialen Kontrolle.

„Appeal to the cautious“: Durch die Stärkung des Sicherheitsgefühls der Bürger begeben sich auch vorsichtige Menschen, die für Straftaten weniger anfällig sind, wieder in den überwachten Bereich.

„Reporting changes“: Um die gewünschte Wirkung von VÜ zu demonstrieren, wird weniger über tatsächlich begangene Straftaten berichtet.[169]

Die sogenannte „Abschreckungsthese“ gilt in der Kriminologie als umstritten, da eine unmittelbar abschreckende Wirkung (Spezialprävention) von VÜ durch empirische Forschungen nicht nachgewiesen werden konnte.[170] Dennoch scheint eine präventive Wirkung der VÜ zumindest aus kriminalitätstheoretischer Perspektive plausibel. Welcher der oben genannten Wirkmechanismen hinter der VÜ öffentlicher Räume steht und ob bzw. unter welchen Voraussetzungen dies im konkreten Anwendungsfall tatsächlich beobachtet werden kann, muss noch erforscht werden.[171]

„Videoüberwachung bedeutet mehr als nur eine Kamera an einem Laternenmast, an einer Hauswand oder in einer Bank – wie Videoüberwachung wirkt, wozu sie genutzt wird und welche weiteren Maßnahmen damit verbunden sind, hängt davon ab, wo und wie sie angewendet wird. Der Kontext der Kameras ist ausschlaggebend, auch für die Einstellung der Menschen zu der Technologie und ihrer möglichen Ausweitung.“[172] Die präventive Wirkungsweise dieses technischen Hilfsmittels steht immer in Konnexion mit einem menschlichen Operator an einem Bildschirm, der aus seiner Beobachtung eine Schlussfolgerung zieht und weitere Maßnahmen einleitet. Als Maßnahme der

---

[169] Vgl. Armitage/Smyth/Pease: Burnley CCTV evaluation in Surveillance of Public Space: CCTV, S. 226 f.
[170] Vgl. Feltes/Kudlacek/Ruch: Schlussbericht zum Verbundprojekt: Analyse von Personenbewegungen an Flughäfen mittels zeitlich rückwärts- und vorwärtsgerichteter Videodatenströme (APFel), S. 6; vgl. Bull: Fehlentwicklungen im Datenschutz am Beispiel der Videoüberwachung, S. 802.
[171] Vgl. Dietrich: Wirksamkeit der polizeilichen Videoüberwachung, S. 11f.
[172] Zurawski: Videoüberwachung in Medien – Macht – Demokratie, S. 7.

Kriminalprävention zielt die VÜ auf die Störung spezifischer Tatgelegenheitsstrukturen ab, nicht aber auf die Beseitigung der grundlegenden Kriminalitätsursachen.[173]

2. IVÜ als Instrument der Kriminalitätsbekämpfung

Wie auch die konventionelle VÜ wäre der Einsatz von intelligenten Systemen der situativen Kriminalprävention zuzuordnen, da auch hier eine Veränderung der Gelegenheitsstruktur bewirkt werden soll. Ein potenzieller Täter soll von seinen Tathandlungen abgeschreckt werden und es soll Einfluss auf die Faktoren genommen werden, die Straftaten begünstigen. Eingesetzte Algorithmen können die kriminalpräventiven Faktoren stärken und den an einem Bildschirm arbeiteten Polizeibeamten unterstützen. Eine einheitliche Aussage, ob und wie intensiv intelligente Systeme Einfluss auf eine präventive Wirkung entfalten, lässt sich aus heutiger Sicht, aufgrund des fehlenden praktischen Einsatzes, nicht sicher sagen. Exemplarisch soll eine Betrachtung für die Möglichkeiten der Objekt-, Gesichts- und Verhaltenserkennung vorgenommen werden.

a) Objekterkennung

Analog der sich bereits im Einsatz befindlichen automatisierten Kfz-Kennzeichenerfassungsgeräten könnte ein objekterkennender Algorithmus für Videokameras im Bereich der kritischen Infrastruktur, wie Flughäfen oder Bahnhöfen, genutzt werden, um bspw. „verdächtige“ Gegenstände zu lokalisieren. Neben dem Einsatz von Schusswaffen ist ein weiterer Modus Operandi islamistischer Terroristen die sog. Kofferbomben (unkonventionelle Spreng- und Brandvorrichtungen, getarnt als Gepäckstücke) auf Bahnhöfen und Flughäfen zu platzieren.[174] Obwohl die Sicherheitskräfte in diesem Bereich sehr sensibel agieren, ist es aufgrund der räumlichen Ausdehnungen solcher Gebäude nahezu unmöglich alle „herrenlosen“ Gepäckstücke zu lokalisieren. Videokameras können indes große Bereiche abdecken.

---

[173] Vgl. Ott: Vorbeugende Überwachung in Kameras gegen Gewalt. Wie effektiv ist die öffentliche Videoüberwachung?, S. 10.

[174] Bsp. Terroranschläge am Flughafen Brüssel-Zaventem 2016; Sprengsatzfund am Bonner Hauptbahnhof 2012; versuchten Bombenanschläge in Köln 2006.

Eine Objekterkennungssoftware kann automatisch abgestellte und somit potenziell verdächtige Gegenstände lokalisieren und einen menschlichen Operator darauf aufmerksam machen. Dieser würde dann weitere Maßnahmen, z.B. Einsatzkräfte zum Ereignisort senden oder aufklären, wie das Gepäckstück an den Ort gelangt ist, ergreifen.

Abbildung 7: Detektierter NZG am Flughafen (in der Mitte des Bildes mit rotem Rahmen gekennzeichnet)[175]

Dem Rational Choice Ansatz folgend müsste ein rational agierender Täter[176] diese Wirkungsweise der VÜ-Technik in seine Tatplanung mit einfließen lassen und könnte zu dem Entschluss kommen, dass ein solcher Anschlag an einem Ort, der mit dieser Technik überwacht wird, aus seiner Sicht zu riskant und daher ungeeignet ist. Selbst wenn er eine mediale Aufmerksamkeit einkalkuliert oder in suizidaler Absicht handelt, so ist zu unterstellen, dass er eine erfolgreiche Tathandlung anstrebt und dass eine frühzeitige Entdeckung seine Pläne gefährden könnte.

---

[175] Bildquelle Fraport AG in Anstädt/Keller/Lutz: Intelligente Videoanalyse, S. 72.
[176] Anmerkung des Verfassers: An dieser Stelle sei einem Täter, der sich mit dem Bau einer USBV befasst, diese als Gepäckstück tarnt und an einem Ort mit hohen Personenaufkommen zur Umsetzung bringen will eine gewisse Rationalität in seinem Vorgehen unterstellt.

Auch nach dem Routine Activity Approach kann konventionelle VÜ Einfluss auf Kriminalität nehmen. Eine stärkere präventive Wirkung kann die intelligente, polizeiliche VÜ im Falle der Objekterkennung entfalten. Auch hier sind die terroristischen Bedrohungslagen an öffentlichen Orten und Plätzen mit erhöhtem Personenaufkommen vorstellbare Einsatzszenarien für die besagte Technik. Diese dürfte nach dem Konzept des Wächters am ehesten zum Tragen kommen, da der Schutz für ein potenzielles Tatobjekt gestärkt wird. Auch eine Wirkung auf den potenziellen Täter könnte denkbar sein, weil sich seine Motivation, eine Straftat zu begehen, durch ein höheres Entdeckungsrisiko bei der Tatvorbereitung, wie dem Abstellen des Koffers, verringert.

Aus Sicht eines potenziellen Opfers ist der Einfluss von Videokameras mit Objektdetektion noch unklarer. Es ist fraglich, ob sich ein potenzielles Opfern risikobewusster verhält, wenn es Kenntnis davon hat, dass VÜ mit intelligenten Systemen ausgestattet sind. Der Effekt der risikobewussteren Umgebungswahrnehmung wird auch bereits mit Videokameras der konventionellen VÜ erreicht. Dem Nutzer des Raumes ist vielleicht gar nicht bewusst, dass Kameras mit intelligenten Funktionen ausgestattet sind. Im ungünstigsten Fall könnte durch den Einsatz eines Algorithmus sogar ein negativer Effekt auftreten, in dem sich das potenzielle Opfer durch die VÜ zu sicher fühlt und dadurch wieder risikoreicher verhält.

b) Gesichtserkennung

Eine zuverlässig funktionierende Gesichtserkennungssoftware kann je nach Zielsetzung ihres Einsatzes eine kriminalpräventive Wirkung entfalten. Wie in Kapitel D beschrieben kann sie zur Identitätsfeststellung oder zur Personenfahndung eingesetzt werden. Dem Rational Choice Ansatz folgend wäre es denkbar, dass ein Täter noch stärker von einer Tat abgeschreckt wird, da eine Zuordnung der Tat, zu seiner Person noch wahrscheinlicher ist. Obwohl die Theorie nur bei rational agierenden Täter zum Tragen kommt, so erstreckt sich die präventive Wirkungsbreite großflächiger, da theoretisch jeder Täter entdeckt werden könnte. *Maximini* sieht in biometrischen Verfahren die größte Schwäche darin, dass sie nur ein eingeschränktes Abschreckungspotenzial haben, da sich das Verfolgungsrisikos bei Tätern nur erhöht, wenn sie bereits

erkennungsdienstlich behandelt wurden.[177] In der Praxis wird der Technik und ihrem Einsatz durch rechtliche Vorgaben Grenzen gesetzt. So ist der Einsatz dieser Technik bei Bagatelldelikten eher unwahrscheinlich (dazu näher in Kapitel F). Ihr Wirkungsgrad wird auch immer in Korrelation zu den Datenbanken stehen, mit Hilfe derer die aufgenommenen Gesichter abgeglichen werden. Neben Fahndungsdatenbanken existieren biometrische Lichtbilder im Personalausweisregister und der Visa- und Asyldatenbanken, auf die beim Vorliegen der Voraussetzungen zurückgegriffen werden könnte.[178] Das würde den Ermittlungsbehörden einen enormen zeitlichen Vorteil verschaffen und die Möglichkeit einräumen, bei entsprechenden Gefährdungslagen Personen aufzuspüren, bevor sie Straftaten begehen. Im Ergebnis wäre in diesen Fällen die kriminalpräventive Wirkung, im Vergleich zur konventionellen VÜ, höher.

Gemäß dem Routine Activity Approach Ansatz könnte die Gefahr einer Viktimisierung durch den Einsatz einer auf gesichtserkennungsbasierender VÜ reduziert werden. Auch hier kann die Technik Einfluss auf das Zusammentreffen der drei Faktoren in räumlicher und zeitlicher Hinsicht nehmen. Die Motivation eines potenziellen Täters könnte durch die gesteigerte Gefahr, identifiziert zu werden, gesenkt oder gänzlich genommen werden. Auch die Schutzmechanismen für ein Tatobjekt dürften durch den Einsatz einer automatischen/ automatisierten Gesichtserkennungssoftware gestärkt werden, da diese Art der Überwachung im Vergleich zur konventionelle VÜ, die immer durch einen menschlichen Beobachter gesichtet und ausgewertet werden muss, permanent und ohne Einbußen in Leistung und Qualität stattfinden. Wie auch bei der Objekterkennung könnte der Einsatz einer intelligenten VÜ auf das potenzielle Opfer einen negativen Einfluss haben, da es sich sicherer fühlt und dadurch zu risikoreicherem Verhaltensmustern neigen kann. In der Gesamtbetrachtung ist ein positiver Einfluss einer intelligenten VÜ durch den Einsatz einer Gesichtserkennungssoftware auf die Kriminalitätsbelastung zu erwarten.

---

[177] Vgl. Maximini: Polizeiliche Videoüberwachung, S. 199.
[178] Exemplarisch: §§ 24, 25 Personalausweisgesetz und § 26 Abs. 4 PAuswG, dass eine bundesweite Datenbank der biometrischen Merkmale nicht errichtet werden soll.

„Aus Sicht der Bundesregierung kann der zielgerichtete Einsatz von Videotechnik [...], dazu beitragen, der staatlichen Verpflichtung zur Prävention und zur Verfolgung von Straftaten nachzukommen. Der Einsatz optisch-elektronischer Sicherheitstechnologie kann präventiv dazu beitragen, die Sicherheit der Bevölkerung zu erhöhen, indem potentielle Täter etwa bei der Erkundung von Örtlichkeiten im Vorfeld oder unmittelbar vor einer Tatbegehung erkannt und diese vereitelt werden kann."[179] Insbesondere die Vorfeldaufklärung seitens der Polizeibehörden kann durch entsprechende Gesichtserkennungsprogramme unterstützt werden. Die biometrischen Gesichtstemplates bekannter Straftäter oder Gefährder[180] könnten in einer Datenbank abgelegt sein, die mit den aufgenommenen Gesichtern aus öffentlichen und potenziell gefährdeten Räumen abgeglichen werden. Bewegt sich eine solche Person im Fokus einer Kamera, so würde das System einen Treffer melden und ein menschlicher Operator könnte weitere Maßnahmen veranlassen. Ein frühzeitiges Einschreiten der Sicherheitsbehörden in das Tatgeschehen wäre möglich und dadurch kann eine Verletzung höherwertiger Rechtsgüter vor einem Schadenseintritt verhindern werden.

c) Verhaltenserkennung

Ohne den weitreichenden Bereich der Verhaltenserkennung näher zu spezifizieren, könnte der Einsatz einer solchen Technik eine ähnliche kriminalpräventive Wirkung entfalten, wie auch die Objektdetektion und die Gesichtserkennung. Darüber hinaus kann es durch den Einsatz von verhaltenserkennender Software in bestimmten Situationen zu einem frühzeitigen Intervenieren durch Sicherheitskräfte kommen, bevor ein Schaden oder eine Schadensvertiefung eintritt. Exemplarisch sind hier das Erkennen einer am Boden liegenden (verletzten oder hilflosen) Person oder das Erkennen einer Kampfsituation

---

[179] Vgl. BT-Drucksache 18/10758, S. 3.

[180] Ein Gefährder ist eine Person, bei der bestimmte Tatsachen die Annahme rechtfertigen, dass sie politisch motivierte Straftaten von erheblicher Bedeutung, insbesondere solche im Sinne des § 100a der Strafprozessordnung (StPO), begehen wird; vgl. D-BT: Legaldefinition des Begriffes „Gefährder", S. 3.

zu nennen (Abb. 8). Das Erkennen von auffälligem und verdächtigenm Verhalten ist derzeit mehr Utopie als Realität und findet daher keine nähere Betrachtung als kriminalitätsbekämpfendes Instrument.

Abbildung 8: Erkennung einer Kampfsituation[181]

d) Fazit

Die konventionelle VÜ kann, wenn man den beiden Kriminalitätstheorien des Rational Choice Ansatz und dem Routine Activity Approach folgt, als Instrument der situativen Kriminalitätsbekämpfung angesehen werden. Sie wirkt aber nur so gut, wie der Mensch vor dem Monitor arbeitet und die Situationen erkennt, richtig einschätzt und weitere Maßnahmen veranlasst. Ihre kriminalpräventive Eigenschaft bleibt auch in vielen Fällen nur solange erhalten, wie potenzielle Täter sie als Risikofaktor für sich einschätzen. Stärke und Dauer der präventiven Wirkung hängen unmittelbar vom menschlichen Zutun ab, dies ändert sich auch durch den Einsatz intelligenter Systeme nicht. „Video-Überwachungssysteme – können als soziotechnische Interaktionen charakterisiert werden, da sie sich grundsätzlich aus einem Zusammenspiel von menschlichen und nicht-menschlichen Akteur_innen konstituieren.“[182] Jedoch kann der Einsatz von technischen Hilfsmitteln, wie der Objektdetektion oder der Gesichts- und Verhaltenserkennung dazu beitragen, dass Gefahrensituationen frühzeitiger und weiträumiger erkannt werden und so eine schnellere Interaktion durch Sicherheitskräfte möglich erscheint. Es können nicht nur konkrete

[181] Bildquelle AxxonSoft in Anstädt/Keller/Lutz: Intelligente Videoanalyse, S. 68.
[182] Egbert/Paul: Zur Einführung in das Themenheft: Über den Mehrwert soziotechnischer Perspektiven für die Kriminologie, S. 87.

Gefahrensituationen frühzeitig erkannt und entschärft werden und dadurch eine generelle kriminalpräventive Stärkung durch die höhere Wirksamkeit entsprechender Systeme eintreten. Wie auch bei der konventionellen VÜ kann die Wirksamkeit situativer Kriminalprävention nur für bestimmte Delikte und Örtlichkeiten unterstellt werden. In Situationen, in denen der Täter emotional gesteuert ist, wie bspw. bei Affekt- und Gewalttaten, kann dieser Ansatz keine Wirksamkeit entfalten.[183] Der wirkliche präventive Nutzen durch den Einsatz intelligenter Systeme der VÜ lässt sich nur durch wissenschaftliche Studien ermitteln. Es ist aber auch hier analog zu den Studien zum Einsatz konventioneller VÜ zu erwarten, dass es zu widersprüchliche Ergebnissen kommen kann.[184] Eine allgemeingültige Aussage über die Effektivität der VÜ als Instrument der Kriminalprävention lässt sich nicht treffen. Gleichwohl kann ihr zumindest eine begrenzte Wirkung unterstellt werden.[185]

Der Einsatz von VÜ im Allgemeinen und von intelligenten Systemen im Besonderen kann zu weiteren Effekten, bspw. einer Verlagerung des unerwünschten Verhaltens, führen.[186] Diese Verlagerung kann eine zeitliche sein, auf eine andere Tatzeit oder eine räumliche Verlagerung in ein anderes Gebiet. Ebenso kann eine Zielverlagerung auf ein anderes Ziel, eine taktische Verlagerung auf einen anderen Modus Operandi in Frage kommen. Weiterhin werden die Verlagerung der Kriminalitätsform auf ein anderes Delikt und die Verlagerung auf einen anderen Täter angeführt. „Nach den Kritikern beuge situative Kriminalprävention Verbrechen nicht vor, sondern führe schlichtweg zu dessen Verlagerung.“[187] Dieser Verlagerungseffekt kann durch den Einsatz von Gesichtserkennungssoftware noch verstärkt werden. Wenn eine Person zu erwarten hat, dass sie weiteren polizeilichen Maßnahmen ausgesetzt ist, weil sie sich in einem Bereich aufhält, der durch Kameras überwacht ist, die

---

[183] Vgl. Tillich: Polizeiliche Videobeobachtung öffentlich zugänglicher Straßen und Plätze in München und Barcelona, S. 35.
[184] Vgl. Lingg: Videoüberwachung im öffentlichen Raum, S. 58.
[185] Vgl. ebd., S. 58.
[186] Vgl. Tillich: Polizeiliche Videobeobachtung öffentlich zugänglicher Straßen und Plätze, S. 36; vgl. Lingg: Videoüberwachung im öffentlichen Raum, S. 34, 58.
[187] Tillich: Polizeiliche Videobeobachtung, S. 36.

einen Abgleich mit einer (Gesichts-) Datenbank vornehmen, so ist anzunehmen, dass sie diesen Bereich meidet, unabhängig davon, ob sie tatsächlich vor hatte, eine delinquente Handlung zu begehen. VÜ hat zum Ziel, dass der Überwachte durch Selbstkontrolle überprüft, ob er sich in dem Raum, in dem er sich bewegt, so verhält, wie es gewünscht ist. Dieser permanente Abgleich vom Soll- mit dem Ist-Zustand wird durch das Gefühl des „Beobachtetwerden" gestärkt. Die überwachte Person ist so angehalten, sich entsprechend den im überwachten Bereich geltenden Regeln (normkonform) zu verhalten. Dieser Effekt könnte durch Algorithmen, die bei einer unerwünschten Verhaltenserkennung weitere Maßnahmen einleiten, verstärkt werden.

Aus Sicht des Überwachten ist es erst einmal unerheblich, ob er durch eine konventionelle oder eine intelligente Kamera überwacht wird. Auch die Unwissenheit verursacht Unsicherheit, die wiederum zu normtreuem Verhalten beitragen kann.[188] Intelligente Systeme erkennen aber frühzeitiger und viel öfter verdächtige Personen, Situationen und Verhaltensweisen und können so gezielt Polizeibeamte an den Einsatzort bringen. Diese kann dann wiederum „eine unmittelbar bevorstehende Straftat noch vor dem tatsächlichen Eintritt in das Versuchsstadium durch indirekte Verhaltenssteuerung mittels Abschreckung und Verunsicherung"[189] abwehren. Intelligente Systeme schaffen die Durchsetzung von Konformität nicht nur auf einer psychischen Ebene, wie die konventionelle VÜ, sondern auch auf einer physischen Ebene, da sie selbstständig detektiert, analysiert und weitere Maßnahmen einleiten kann.[190] Analysiert man die situative Präventionsstrategie der VÜ, so stellt man fest, dass es auch zu positiven Nebeneffekten kommen kann.[191] Die sogenannte „diffusion of benefits"[192] zeigt eine stärkere präventive Wirkung, auch an Orten und zu Zeiten, an denen die eigentliche Maßnahme gar nicht aktiviert ist.[193] Der Effekt, der Ausbreitung vorteilhafter Wirkungen, kann zumindest theoretisch

---

[188] Vgl. Stolle: Situative Kriminalprävention, S. 182.
[189] Stolle: Situative Kriminalprävention, S. 182.
[190] Ebd., S. 182.
[191] Vgl. Tillich: Polizeiliche Videobeobachtung öffentlich zugänglicher Straßen…, S. 36.
[192] Übersetzung des Verfassers: „Ausbreitung vorteilhafter Wirkungen".
[193] Vgl. Tillich: Polizeiliche Videobeobachtung öffentlich zugänglicher Straßen…, S. 39; vgl. Maximini: Polizeiliche Videoüberwachung, S. 16.

durch den Einsatz von intelligenten Videoüberwachungssystemen verstärkt werden. Ursächlich hierfür könnte ein starker Glaube an die technische Wirksamkeit aber auch das tatsächliche frühzeitigere Agieren von Sicherheitskräften an den überwachten Örtlichkeiten sein.

II VÜ zur Verbesserung der Strafverfolgung

Das Ziel von VÜ ist primär die präventive Verhinderung von Straftaten. Erst im zweiten Schritt soll die VÜ bei der Aufklärung von Straftaten unterstützen.[194] Die Verfolgung von Straftaten fällt genauso wie die polizeiliche Vorbeugung in den Bereich der Kriminalistik, da sich durch eine systematische, technische Observation eine verbesserte Verfolgungs- und Aufklärungsmöglichkeit gewährleistet wird.[195]

1. Konventionelle VÜ als Hilfsmittel repressiver Polizeiarbeit

Die Effektivität der VÜ zur Aufklärung von Straftaten kann anhand der Auswertung der durch VÜ initiierten Einsätze und sonstiger interner Auswertung nachvollzogen werden.[196] So kam es im Bereich der Landespolizei Hessen in den letzten fünf Jahren durch die Beobachtung der Videomonitore „zur Feststellung/ Beobachtung von 813 strafrechtlich relevanten Sachverhalten, die entsprechende Fahndungs-, Festnahme- oder Identifizierungsmaßnahmen zur Folge hatten."[197] Es ist zu beachten, dass die Repressionsfunktion der VÜ je nach konkreter Nutzung mehrdimensional ist. So kann eine Straftat über den Monitor durch einen Beobachter wahrgenommen werden oder die vor Ort befindlichen Polizisten können durch die Aufschaltung von Kameras an dem Ereignisort unterstützt werden. Zudem können gespeicherte Aufnahmen als Beweismittel in Strafverfahren verwendet und die visuelle Fahndung nach Personen unterstützt werden.[198] Voraussetzung hierfür ist neben einer technischen Ausstattung, die es ermöglicht, eine entsprechende Bildqualität und räumliche Streubreite zu liefern, ein „reaktives Konzept, dass eine zeitnahe Intervention

---

[194] Vgl. Lingg: Videoüberwachung im öffentlichen Raum, S. 42.
[195] Vgl. Büllesfeld: Polizeiliche Videoüberwachung, S. 63.
[196] Vgl. Lingg: Videoüberwachung im öffentlichen Raum, S. 47.
[197] HLKA: Handlungsempfehlung für die Errichtung und den Betrieb von Videoüberwachungsanlagen im öffentlichen Raum, S. 7.
[198] Vgl. Lingg: Videoüberwachung im öffentlichen Raum, S. 47.

sicherstellt."[199] Die konventionelle VÜ ist als Hilfsmittel repressiver Polizeiarbeit nur so gut wie der menschliche Beobachter, der das Videomaterial sichtet. Polizeiliche Videoüberwachung öffentlicher Räume kann daher immer nur ein selektiver Blick als eine ubiquitäre Überwachung sein.[200] Und dennoch sind gerade repressive Erfolge durch Öffentlichkeitsfahndung gem. § 131b StPO oder Festnahmen aufgrund von Videokameras aufgezeichneter Täter sowie Verurteilungen im Strafverfahren durch Videobeweise wichtig, da sie eine messbare Größe darstellen und die Maßnahme der VÜ als solche in der Öffentlichkeit eine Legitimation erhält.[201]

2. IVÜ als Hilfsmittel repressiver Polizeiarbeit

In vielen Fällen werden Täter und Tathandlungen durch Überwachungskameras videografiert, weil sie sich aus unterschiedlichen Gründen nicht durch Videokameras haben abschrecken lassen. Die Auswertung der Videodaten und Zuordnung von Personen zu Tathandlungen ist vielmals ein (zeitliches) Nadelöhr für die Ermittler. Auch ist eine Identifizierung von Tatverdächtigen in vielen Fällen nur durch die Hilfe der Öffentlichkeit möglich, was für einen Tatverdächtigen einen nicht unerheblichen Eingriff in seine Grundrechte und eine lebenslange Stigmatisierung bedeuten kann, gleichwohl ob er rechtskräftig verurteilt wird oder nicht. Die vielfältigen Einsatzmöglichkeiten intelligenter Systeme, wie die Analyse von Videomassedaten und die automatisierte Personenfahndung durch Gesichtserkennungsalgorithmen können „die Ermittlung von Tatverdächtigen beziehungsweise die Überführung von Tätern erleichtern und somit eine tertiär kriminalpräventive Wirkung entfalten."[202] Zudem stünde den Ermittlern die Möglichkeit von automatisiertem Personenfahndungen an neuralgischen Punkten zur Verfügung, wenn eine Software mit Gesichtserkennung und automatischen Datenabgleich mit einer Fahndungsdatenbank eingesetzt werden würde. Die polizeiliche Arbeit könnte durch den Einsatz intelligenter VÜ noch effizienter werden und so zu einer Verbesserung der Strafverfolgung führen.

---

[199] Stolle: Situative Kriminalprävention, S. 184.
[200] Vgl. ebd., S. 185.
[201] Vgl. Lingg: Videoüberwachung im öffentlichen Raum, S. 47.
[202] Müller: Mehr Kameras für mehr Sicherheit?, S. 310.

III VÜ zur Stärkung des Sicherheitsgefühls der Bevölkerung

Der VÜ wird neben der Verhinderung und Aufklärung von Straftaten eine dritte primäre Eigenschaft zugesprochen: die Stärkung des (subjektiven) Sicherheitsgefühls in der Bevölkerung.[203] Unter dem Begriff „Subjektives Sicherheitsgefühl“[204] versteht man die individuelle Einschätzung des Einzelnen zu seiner Sicherheit bzw. wie hoch er die Gefahr sieht, dass seine Rechtsgüter beeinträchtigt werden. Das subjektive Sicherheitsgefühl wird oftmals mit dem kriminologischen Begriff der Kriminalitätsfurcht/ -angst („fear of crime“) gleichgesetzt, da als Hauptursache der befürchteten Rechtsgüterbeeinträchtigung eine zunehmende Kriminalität angenommen wird. Das subjektive Sicherheitsgefühl geht aber über die Kriminalitätsfurcht hinaus. Das Sicherheitsgefühl erfasst auch Bedrohungen, die nicht nur aus eine Besorgnis vor eigenen unmittelbaren Gefährdungen durch Kriminalität hervorgehen.[205] Es steht nicht in unmittelbaren Zusammenhang zur tatsächlichen Wahrscheinlichkeit, Opfer einer Straftat zu werden, sondern ist in hohem Maße von individuellen und gesellschaftlichen Faktoren abhängig.[206]

Untersuchungen zur sozialen und personalen Furcht kommen zu zwei Feststellungen. Auf der einen Seite fällt die allgemeine Besorgnis über die gesellschaftliche Bedrohung durch Kriminalität regelmäßig höher aus als die konkrete Besorgnis, persönlich Opfer von Kriminalität zu werden. Auf der anderen Seite ist die Angst vor steigender Kriminalität der Hauptgrund für die allgemeine Besorgnis. Die individuelle Viktimisierungserwartung spielt dagegen eine eher untergeordnete Rolle.[207] Die Divergenz von Ursachen der Kriminalitätsfurcht ist in Gänze kaum beeinflussbar und daher scheint es fraglich, ob sich durch konkrete Maßnahmen, wie der VÜ, das Sicherheitsgefühl steigern lässt.[208]

---

[203] Vgl. Hornung/Desoi: "Smart Cameras" und automatische Verhaltensanalyse, S. 153; vgl. BT-Drucksache 18/10758, S. 3.
[204] In der Kriminologie wird der Begriff „Kriminalitätsfurcht“ auch an der Stelle des „Sicherheitsgefühls“ verwendet, vgl. Lingg: Videoüberwachung im öffentlichen Raum, S. 53.
[205] Vgl. Rothmann: Sicherheitsgefühl durch Videoüberwachung?, S. 104; vgl. Schewe: Subjektives Sicherheitsgefühl in Wörterbuch zur Inneren Sicherheit, S. 322.
[206] Vgl. Maximini: Polizeiliche Videoüberwachung, S. 16.
[207] Vgl. Hummelsheim-Doss: Objektive und subjektive Sicherheit in Deutschland, S. 36.
[208] Vgl. Maximini: Polizeiliche Videoüberwachung, S. 17.

	Individuelle:	Soziale:
Kognitiv	- Viktimisierungserwartung und persönliche Bewertung der Folgen	- Sorge über die allgemeine Wahrscheinlichkeit, dass jemand Opfer einer Straftat wird
Affektiv	- Unsicherheitsgefühl	- Sorge über die Kriminalitäts-belastung in Deutschland
Konativ	- Abwehrmaßnahmen bzw. Vermeidungsverhalten	- Erwartung an den Staat, die Kriminalitätsrate zu senken

Abbildung 9: Dimensionen der Kriminalitätsfurcht[209]

Verschiedene Studien kommen zu unterschiedlichen Ergebnissen im Hinblick auf den Einfluss der Kriminalitätsfurcht durch den Einsatz von Videokameras. Einige Studien stellen fest, dass VÜ tatsächlich das Sicherheitsgefühl der Bevölkerung stärken kann.[210] Andere hingegen kamen zu dem Ergebnis, dass VÜ kaum Einfluss auf das Sicherheitsgefühl hat.[211] Teilweise führte die Installation von Videokameras dazu, dass auf Unsicherheit hingewiesen wurde und dadurch neue Ängste geschaffen wurden, anstatt sie zu verhindern.[212]

VÜ, unerheblich, ob es sich um den Einsatz von konventioneller VÜ oder dem Einsatz intelligenter Systeme handelt, ist kein probates Mittel, das subjektive Sicherheitsgefühl in der Bevölkerung zu stärken. Dies kann auf verschiedene Faktoren zurückgeführt werden. Das subjektive Sicherheitsgefühl lässt sich nicht exakt auf einen überwachten Raum beschränken, zum anderen ist die Kriminalitätsbelastung an den bewachten Orten empirisch nicht sehr hoch, so dass diese nicht als Angsträume angesehen wurden. Personengruppen, die durch Kriminalitätsfurcht besonders belastet sind, wie ältere Menschen, meiden diese Räume, so dass eine Senkung dieser Furcht von vornherein ausgeschlossen ist.[213] Ein weiterer Ansatz ist, dass der VÜ anfänglich eine höhere Wirksamkeit zugetraut wird, als sie tatsächlich im Stande ist zu leisten und

---

[209] Nach Schwind, Kriminologie, § 20, S. 429 und Reuband: Kriminalitätsfurcht in Auf der Suche nach neuer Sicherheit, S. 238.
[210] Vgl. ebd., S. 60; vgl. Lingg: Videoüberwachung im öffentlichen Raum, S. 56; vgl. Müller: Mehr Kameras für mehr Sicherheit?, S. 309.
[211] Vgl. ebd., S. 61; vgl. Lingg: Videoüberwachung im öffentlichen Raum, S. 57; Vgl. Müller: Mehr Kameras für mehr Sicherheit?, S. 309.
[212] Vgl. Lingg: Videoüberwachung im öffentlichen Raum, S. 56.
[213] Vgl. Müller: Mehr Kameras für mehr Sicherheit?, S. 309.

dass dieses Vertrauen in die Technik mit der Zeit nachlässt. So wie die abschreckende Wirkung bei potenziellen Tätern mit der Zeit nachlässt, so meiden die Menschen entsprechende Orte nach einer gewissen Zeit wieder mehr. „So könnte sich das Verhalten der Bürger als Spiegelbild des Verhaltens der wieder ermutigten Täter erklären."[214]

Trotz dieser Erkenntnisse aus verschiedenen nationalen und internationalen empirischen Studien wird dennoch der Ausbau der VÜ mit der Begründung, dass das Sicherheitsgefühls der Bevölkerung gestärkt werden muss, vorangetrieben. Immer häufiger dient das subjektive Sicherheitsgefühl als Rechtfertigung staatlicher Maßnahmen, obwohl die objektive Sicherheitslage so geringe Auswirkungen auf das subjektive Sicherheitsgefühl hat.[215] Sicherheitspolitiker nutzen die von der großen Mehrheit falsch eingeschätzte Kriminalitätsentwicklung und individuellen Bedrohungslage aus.[216] Sie können so Maßnahmen ergreifen, die „weniger darauf abzielen, die objektive Sicherheit zu stärken, als vielmehr der Bevölkerung das Gefühl zu vermitteln, es werde alles für ihre Sicherheit unternommen."[217] Begünstigt wird dieser Kurs dadurch, dass das subjektive Sicherheitsempfinden nicht mehr nur von der Furcht vor Kriminalität beeinträchtigt wird, sondern auch von der Furcht vor terroristischen Anschlägen. „Allein die Grundidee des Terrors, durch die Unvorhersehbarkeit und Allgegenwärtigkeit der Gefahr eines Anschlags Furcht unter der Bevölkerung zu verbreiten, erklärt die Wirkung auf das subjektive Sicherheitsgefühl. Ihre Beeinträchtigung ist das Ziel des Terrorismus und nicht bloße Nebenfolge, wie bei der Kriminalität."[218] Wohl auch deshalb wird der Ausbau von Videoüberwachung auch immer mit dem Kampf gegen den Terrorismus begründet.

Die von empirischen Befunden über die Effektivität der VÜ zur Steigerung des subjektiven Sicherheitsgefühls in der Bevölkerung scheinbar losgelöste Ver-

---

[214] Maximini: Polizeiliche Videoüberwachung, S. 61.
[215] Vgl. Schewe: Subjektives Sicherheitsgefühl in Wörterbuch zur Inneren Sicherheit, S. 324.
[216] Vgl. Reuter: Zwei Drittel der Deutschen schätzen Kriminalitätsentwicklung falsch ein, auf https://netzpolitik.org/2016/repraesentative-umfrage-zwei-drittel-der-deutschen-schaetzen-kriminalitaetsentwicklung-falsch-ein/, abgerufen am 04.01.2018.
[217] Schewe: Subjektives Sicherheitsgefühl in Wörterbuch zur Inneren Sicherheit, S. 325.
[218] Ebd., S. 325.

breitung von VÜ als sicherheitspolitische Maßnahme, wird auch als ein grundsätzlicher Wandel der Kriminalpolitik verstanden. „Die globalisierte und deregulierte Marktwirtschaft, der sukzessive Abbau wohlfahrtsstaatlicher Sicherungsmechanismen, eine verstärkte Individualisierung und Pluralisierung von Lebensstilen sowie eine allgemeine Normerosion und ein zunehmender Verlust traditioneller Erwartungssicherheiten im alltäglichen Handeln begünstigen auch die Etablierung neuer Praktiken sozialer Kontrolle.“[219] Insbesondere medial aufbereitete internationale terroristische Bedrohungsszenarien schüren einen (Un-)Sicherheitsdiskurs und führen dadurch zur Etablierung diverser sicherheitstechnischer Interventionen, wie den Ausbau der VÜ, ohne einen Nachweis über die Effektivität zu erbringen.[220]

Für die Verantwortlichen in der Politik ist die VÜ ein leicht einsetzbares sicherheitstechnologisches Instrument, um in offensichtlicher Weise auf gesellschaftliche Verunsicherungen zu reagieren.[221] Der Staat stillt so das soziale Bedürfnis nach Sicherheit.[222] So lässt sich neben dem Ausbau weiterer Videokameras auch die Etablierung intelligenter Systeme begründen. Die Erwartungshaltung und der Glaube an die Wirksamkeit neuer Technologien zur Erreichung von Sicherheit als angestrebtes Ziel ist hoch. Doch Sicherheit ist eine „diffuse Variable auf einer Skala ohne natürliche Obergrenze, was letztlich dazu führt, dass immer ein gewisses Restrisiko bestehen bleibt und totale Sicherheit nie erreicht werden kann.“[223]

---

[219] Rothmann: Sicherheitsgefühl durch Videoüberwachung?, S. 106.
[220] Vgl. ebd. S. 106.
[221] Vgl. Rothmann: Sicherheitsgefühl durch Videoüberwachung?, S. 106.
[222] Vgl. Reuband: Kriminalitätsfurcht in Auf der Suche nach neuer Sicherheit, S. 238.
[223] Ebd., S. 106.

IV Die Reduzierung von Kosten für die Überwachung von Objekten und Räumen durch Personaleinsparungen

Neben den drei Primärzielen der VÜ wird bei ihrer Etablierung auch gerne mit der Reduzierung von Kosten für die Überwachung von Objekten und Räumen durch Personaleinsparungen argumentiert. Für beide Verfahren der VÜ entstehen anfänglich Kosten für die Beschaffung, die Installation und Umrüstung. Hinzu kommen laufende Kosten für Wartung, Strom und Reparaturen.[224]

1. Reduzierung von Personalkosten durch konventionelle VÜ

Videoüberwachung ist aber nur effizient, wenn sie auch ausgewertet wird. Dies kann im Falle der konventionellen VÜ durch eine Live-Beobachtung oder eine spätere Sichtung von Aufzeichnungen geschehen. Neben Investitionen in die Technik muss auch in Mitarbeiter investiert werden, dass die Videobilder auswertet und die für etwaige Interventionen zur Verfügung steht.[225] Die Autoren *Bücking* und *Kubera* stellten in ihrer Evaluation der VÜ fest, dass der Einsatz von Videokameras insgesamt kein Personal einspart, aber dessen Einsatz effizienter gestaltet werden kann. Sie kommen zu dem Entschluss, dass aufgrund der hohen Kosten für Personal und Technik VÜ nur an Kriminalitätsbrennpunkten ökonomisch sinnvoll ist und auch nur dann, wenn Personal zur Intervention vor Ort zur Verfügung steht. Nur so kann sichergestellt werden, dass im Einsatzfall möglichst schnell interagiert wird und die VÜ ihre präventive Wirkung nicht verliert. Parallel stellt die VÜ ein objektives Beweismittel für die nachträgliche Ermittlungsarbeit dar.[226] *Maximini* kommt zu dem Entschluss, dass der Hauptkostenfaktor bei der VÜ immer noch die Beobachtung und Auswertung des Videomaterials durch den Menschen ist.[227]

---

[224] Vgl. Maximini: Polizeiliche Videoüberwachung, S. 62.
[225] Vgl. ebd., S. 62.
[226] Vgl. Bücking/Kubera: „Eine digitale Streifenfahrt…“, S. 305 ff.
[227] Vgl. Maximini: Polizeiliche Videoüberwachung, S. 198.

2. Reduzierung von Personalkosten durch den Einsatz intelligenter Systeme

Wie in den verschiedenen Einsatzmöglichkeiten vorgestellt, liegt die Leistungsfähigkeit intelligenter Systeme darin, automatisiert Videodaten zu analysieren. Gerade dieser Schritt der Auswertung ist der zeit- und personalintensivste. Obwohl die eigentliche Identifikation oder Entscheidung über weitere Maßnahmen durch einen menschlichen Operator fällt, so ist eine Kostenreduzierung durch Personaleinsparungen für die Sichtung und Analyse der Daten wahrscheinlich.[228] Wirkungsvoll bleibt die Maßnahme aber nur, wenn Personal für Interventionen und Anschlussmaßnahmen bereitgehalten wird.[229]

V Disziplinierung der Verhaltensweisen der Nutzer der beobachteten Räume

Die Disziplinierung der Verhaltensweisen der Nutzer der beobachteten Räume gilt als ein Ziel der VÜ und ist zugleich auch einer der strittigsten Punkte. Während gewisse Verhaltensänderungen/-anpassungen durchaus wünschenswert sind, so stellen andere Verhaltensweisen eine ungewollte Nebenwirkung dar.[230] Eine gewollte Verhaltensänderung könnte durch die bewusste Wahrnehmung der Videokameras geschehen. Dadurch soll, nach dem Routine Activity Approach, bei dem potenziellen Opfer ein risikobewussteres Verhalten eintreten, so dass sie kein geeignetes Zielobjekt/ Opfer mehr darstellt.[231] Aber auch die Abschreckungsthese bei einem potenziellen Täter und der Ansatz „Publicity“, der durch eine mediale Berichterstattung zum Thema VÜ den Bürger zu gesetzeskonformem Verhalten ermutigt, kann eine gewollte Disziplinierung der Verhaltensweisen darstellen.[232] Ob der Einsatz intelligenter Systeme im Vergleich zur konventionellen VÜ die gewünschten Wirkungen verstärken kann, lässt sich aus heutiger Sicht nur spekulativ beantworten. Zu den negativen Auswirkungen von Verhaltensänderungen durch den Einsatz von intelligenter VÜ wird an dieser Stelle auf das Kapitel G verwiesen.

---

[228] Vgl. Maximini: Polizeiliche Videoüberwachung, S. 199.
[229] Vgl. Bücking/Kubera: „Eine digitale Streifenfahrt…“, S. 306.
[230] Vgl. Koch/Held/u.a.: Intelligente Videoüberwachung: eine Handreichung, S. 20.
[231] Vgl. Tillich: Polizeiliche Videobeobachtung öffentlich zugänglicher Straßen, S. 34.
[232] Vgl. Armitage/Smyth/Pease: Burnley CCTV evaluation in Surveillance of Public Space: CCTV, S. 226 f.

VI Zusammenfassung

Im Hinblick auf die konventionelle VÜ konnte durch die empirische Forschung bislang kein eindeutiger Beweis darüber erbracht werden, dass VÜ eine besondere präventive bzw. repressive Wirkung hat bzw. dass eine Steigerung des Sicherheitsgefühls in der Bevölkerung festzustellen ist.[233] Die Auswertung von Literatur zu Pilotprojekten und Evaluationsstudien zeigt ein differenziertes Bild der VÜ. So wurden in einigen Projekten gute Erfolge erzielt, indem ein Nachweis über die Wirkung erbracht wurde und in anderen Projekten wurden nur wenige oder überhaupt keine Wirkungen erzielt.[234] Eine allgemeingültige Aussage über die Wirksamkeit konventioneller polizeilicher VÜ öffentlich zugänglicher Orte lässt sich nicht treffen. VÜ steht im Kontext mit anderen Maßnahmen und Faktoren, die den Effekt in positiver oder negativer Weise beeinflussen können.[235] Dennoch erfährt VÜ eine hohe Akzeptanz bei den verantwortlichen Entscheidungsträgern und der Bevölkerung. Ausschlaggebend scheint hier nicht die tatsächliche Wirksamkeit zu sein, sondern vielmehr die der Technik zugeschriebene Wirkung.[236]

Im Bereich intelligenter Systeme lassen sich im Hinblick auf die präventive Wirkung, insbesondere auf der subjektiven Ebene, bzw. zur Steigerung des subjektiven Sicherheitsgefühls nur theoretische Überlegungen anstellen, da aufgrund des fehlenden praktischen Einsatzes keine Evaluationsstudien vorliegen. Ihre Wirkung ist zumindest aus heutiger Sicht fraglich. Die Stärke dieser Systeme liegt in der automatischen Detektion und Auswertung, dadurch sind konkrete Szenarien denkbar, in denen ein(e) Schadenseintritt/-vertiefung durch eine schnellere Intervention von Sicherheitskräften verhindert werden kann, da konkrete Gefahrensituationen eher erkannt werden. Beispielhaft sind hier das Abstellen eines als Koffer getarnte USBV bzw. die Möglichkeit der Gesichtserkennung und des Datenabgleichs mit einer „Gefährder“ -Datenbank

---

[233] Vgl. Dietrich: Wirksamkeit der polizeilichen Videoüberwachung, S. 65; vgl. Feltes/Kudlacek/Ruch: Schlussbericht zum Verbundprojekt: Analyse von Personenbewegungen an Flughäfen mittels zeitlich rückwärts- und vorwärtsgerichteter Videodatenströme (APFel), S. 6; vgl. Apelt/Möllers: Wie „intelligente“ Videoüberwachung erforschen?, S. 586.
[234] Vgl. Dietrich: Wirksamkeit der polizeilichen Videoüberwachung, S. 91.
[235] Vgl. ebd., S. 92.
[236] Vgl. ebd., S. 65.

zu nennen. Diese Möglichkeiten könnten Straftaten verhindern noch bevor sie begangen werden bzw. noch vor dem tatsächlichen Eintritt in das Versuchsstadium.[237] Dies würde im Gegensatz zur konventionellen VÜ einen klaren Mehrwert im Bereich der Kriminalprävention zur Vorbeugung rechtswidriger Taten darstellen. Da die Technik aber nur punktuell an klar definierten Orten zum Einsatz kommt, könnten diese von Personen gemieden werden, die darüber Kenntnis haben, dass sie eventuell einen Trefferfall darstellen könnten.

Der höchste Nutzwert durch den Einsatz intelligenter Systeme der VÜ ist als Hilfsmittel in der repressiven Polizeiarbeit zu sehen, da die VÜ nicht mehr nur stiller Beobachter ist, sondern selbstständig detektieren, analysieren und Datenabgleiche vornehmen kann. Je nach Algorithmus und Einsatz der Technik können Personen identifiziert und Tathandlungen schneller und eindeutiger den potenziellen Tätern zugeordnet werden. Auch die Fahndung nach Straftätern kann durch den Einsatz von Gesichtserkennungssoftware unterstützt werden. Die vielfältigen Einsatzmöglichkeiten dieser Technologie könnten für die Sicherheitsbehörden eine enorme Zeit- und Personaleinsparung bedeuten und dennoch effizienter sein, als der Einsatz der heutigen konventionellen VÜ.

Damit einhergehend ist eine Kostenreduzierung durch die Einsparung von Personal, welches die Beobachtung und Auswertung von Videoaufnahmen zur Aufgabe hat, verbunden. Auch wenn die Überwachung öffentlicher Plätze durch Videokameras heute schon mehr ist als eine bloße technische Komponente zur Unterstützung der Polizeiarbeit,[238] so kann davon ausgegangen werden, dass die Einführung weiterer intelligenter Systeme die präventive und insbesondere die repressive Polizeiarbeit vereinfachen wird und darüber hinaus Einfluss auf die zukünftige Kriminalitätsentwicklung und die Gesellschaft nehmen wird. Voraussetzungen dafür wären neben der rechtlichen Zulässigkeit die Legitimation durch die Bevölkerung.

---

[237] Vgl. Stolle: Situative Kriminalprävention, S. 182.
[238] Vgl. Dietrich: Wirksamkeit der polizeilichen Videoüberwachung, S. 92.

F Zulässigkeit und Legitimation des polizeilichen Einsatzes „intelligenter“ VÜ öffentlich zugänglicher Räume

Der Einsatz konventioneller VÜ durch staatliche Stellen findet sich in bundes- und landesgesetzlichen Normierungen wieder und kann in gefahrenabwehr- und strafverfolgungsrechtliche Ermächtigungsgrundlagen unterschieden werden.[239] Ermächtigungsgrundlagen sind immer dann nötig, wenn durch oder auf Grund eines Gesetzes ein Grundrecht eingeschränkt wird. Diese Arbeit folgt der These, dass es durch den Einsatz von intelligenten System in der VÜ zur Einschränkung von Grundrechten kommt, die durch die derzeitigen Ermächtigungsgrundlagen nicht ganzheitlich legitimiert sind. Diese wäre immer dann der Fall, wenn der Sprung von der konventionellen zur intelligenten VÜ mehr als nur ein gradueller Entwicklungsschritt wäre.[240]

Der technische Fortschritt einer iVÜ ist aber mehr als eine unwesentliche Weiterentwicklung der konventionellen VÜ. Er ermöglicht, menschliche Aufgaben zu übernehmen, beispielsweise das Erkennen von Gesichtern oder eines bestimmten Verhaltens.[241] Die in Kapitel C beschriebenen Verfahren der Videoanalyse sind als automatisierte Datenverarbeitung anzusehen. „Gegenüber der einfachen Videoüberwachung resultieren daraus die grundrechtsdogmatischen Unterschiede eines zusätzlichen Eingriffs und der erhöhten Eingriffsintensität durch die intelligente Bildanalyse. Dies muss zumindest dann gelten, wenn die Daten nicht anonymisiert erhoben werden.“[242]

Held skizziert zwei Gruppierungen rechtlicher Fragestellung. Im ersten Problemkomplex steht die Beeinträchtigung von Grundrechten durch die Überwachung und im zweiten geht es um die Legitimation von Algorithmen als Entscheider. Hierunter versteht er, dass durch die Technisierung „Entscheidungen abstrakt und generell getroffen werden müssen, die zuvor ein menschlicher Anwender im Einzelfall fällen konnte.“[243] Da Algorithmen vor dem Einsatz programmiert werden müssen, müssen auch die Kriterien der Entscheidung

---

[239] Vgl. Starnecker: Videoüberwachung zur Risikovorsorge, S. 31.
[240] Vgl. ebd. S. 48.
[241] Vgl. Held: Intelligente Videoüberwachung, S. 63; vgl. Stettner: Sicherheit am Bahnhof, S. 139.
[242] Held: Intelligente Videoüberwachung, S. 54.
[243] Vgl. Held: Intelligente Videoüberwachung, S. 31f.

ohne Bezug zu einem Einzelfall definiert werden. Während bei der konventionellen VÜ ein menschlicher Beobachter jeden konkreten Einzelfall betrachtet und beurteilt und Entscheidungen aufgrund seiner Erfahrungen trifft, entscheidet eine Software nach statistischen Verfahren.[244]

In den Kapiteln B und C wurde dargestellt, dass es nicht *die* eine intelligente Videoüberwachung gibt, sondern dass sich verschiedene Verfahren mit unterschiedlicher Eingriffsintensität darunter subsumieren lassen. Im Nachfolgenden soll nun geprüft werden, zu welchen Grundrechtseinschränkungen und in welcher Intensität es durch die verschiedenen Verfahren kommt und welche Rechtsgrundlagen hierfür erforderlich wären. Unterschieden werden hierbei die automatisierte Kfz-Kennzeichenerfassung sowie die Mustererkennung mit und ohne Personenbezug.

I Automatisierte Kfz-Kennzeichenerfassung

Die „automatisierte Kennzeichenerfassung“[245] ist die derzeit einzige polizeiliche und gesetzlich normierte Maßnahme, die selbstständig Daten erhebt, verarbeitet und abgleicht und somit die technischen Eigenschaften einer intelligenten VÜ erfüllt.[246] Die Maßnahme der Kennzeichenerfassung besteht aus mehreren Einzeleingriffen. Da diese aber nur in der Gesamtheit die Maßnahme überhaupt ermöglichen, werden sie zusammen betrachtet.

1. Eingriffsintensität automatisierter Kfz-Kennzeichenerfassung

Um festzustellen, ob und in welcher Intensität die Maßnahme der automatisierten Kennzeichenerfassung Grundrechte einschränkt, muss zwischen einem Nicht-Treffer, einem Treffer und einem Fehltreffer unterschieden werden. Laut Bundesverfassungsgericht liegt kein Eingriff in das Recht der informationellen Selbstbestimmung (Art. 2 Abs. 1 GG in Verbindung mit Art. 1 Abs. 1 GG) vor, solange die automatisch erhobenen Kfz-Kennzeichen nach fehlender Übereinstimmung mit den Fahndungsdatenbanken „sofort,

---

[244] Vgl. Held: Intelligente Videoüberwachung, S. 31f.
[245] BVerfG, Urt. vom 11.03.2008 Az. 1 BvR 2074/05, 1254/07.
[246] Vgl. Stettner: Sicherheit am Bahnhof, S. 115f.

anonym und spurenlos wieder gelöscht werden […], ohne dass eine Verwertung dieser personenbezogenen Daten möglich ist.“[247] Entscheidend ist hierbei das die Daten zwar zielgerichtet erfasst und verwertet werden, sie aber bei einem Nicht-Treffen das geschlossene Computersystem nicht verlassen. Es besteht so keine Gefahr, dass erhobene Informationen weitergegeben werden und somit ist eine „Gefährdung für die Persönlichkeit des Betroffenen durch eine Preisgabe von Daten“[248] ausgeschlossen.

Durch die technischen Geräte der Kennzeichenerfassung könnte bei den Betroffenen ein Gefühl der Beobachtung vermittelt werden, was zu Einschüchterungseffekten und dadurch zu einer Verhaltensänderung führen kann. Diese könnte eine Beeinträchtigung des allgemeinen Persönlichkeitsrechts gem. Art 2 Abs. 1 GG darstellen. Bei der Maßnahme der Kennzeichenerfassung lässt sich aber vermuten, dass, wenn eine solche Einschüchterung vorliegt, sie nicht sonderlich intensiv sein wird. Es lässt sich anführen, dass die Geräte zwar Kennzeichen offen erfassen, aber dieser Eingriff durch den Betroffen nicht registriert wird, da die Geräte keine Rückmeldung in Form von Blitzen oder dergleichen geben. Zudem sind die Möglichkeiten der Datenerfassung auf die Kennzeichen beschränkt. Es können rein technisch keine Personen (-daten) erfasst werden. Dies ist zumindest nicht allen Betroffenen bewusst und so kann auch „die Ungewissheit über Erhebung und Verwendung der Daten und die Art der vermeintlich oder tatsächlich erhobenen Daten […] Kriterien zur Bestimmung der Intensität der Einschüchterung sein.“[249] Da es derzeit noch keine Evaluationsstudien zum Einschüchterungseffekt durch Kfz-Kennzeichenerfassungsgeräte gibt, ist die Intensität der Grundrechtseinschränkung durch Einschüchterungseffekte rein spekulativ.[250]

Im Falle eines Treffers bzw. eines Fehlalarms liegt ein Eingriff in das Recht auf informationelle Selbstbestimmung vor, da hier bei einer Übereinstimmung der erfassten Kennzeichen mit einer Ausschreibung in einer Fahndungsdatenbank

---

[247] Stettner: Sicherheit am Bahnhof, S. 116; BVerfG, Urt. vom 11.03.2008 Az. 1 BvR 2074/05, 1254/07.
[248] Ebd., S. 117.
[249] Stettner: Sicherheit am Bahnhof, S. 118; S. 72f.
[250] Vgl. ebd., S. 118.

die Daten nicht nur erfasst, sondern speichert und so für eine weitere Verwendung zur Verfügung stehen. Ein Eingriff in das Recht auf informationelle Selbstbestimmung liegt nach dem Bundesverwaltungsgericht bereits schon bei einer Gefährdung der Persönlichkeit und Freiheit vor.[251] Dies ist gegeben, sobald Informationen für Behörden verfügbar gemacht werden und sie das geschlossenen Computernetzwerk verlassen bspw. als Treffermeldung einem menschlichen Entscheider aufgezeigt werden.[252] Hierbei ist es unerheblich, ob es sich um einen wirklichen Treffer mit dem Fahndungsbestand handelt oder um einen Fehlalarm.[253] Auch ist es unerheblich, dass nur das Kfz-Kennzeichen erfasst wird, denn die Erhebung von Daten mit „für sich genommen nur geringem Informationsgehalt“[254] geben die Möglichkeit für eine Weiterverarbeitung, wie einer Halterabfrage.[255] Der durch die Maßnahme stattfindende Eingriff in das Recht auf informationelle Selbstbestimmung ist durch die Erfassung großer Datenmengen in kurzer Zeit[256] und den automatisierten Datenabgleich mit einem hohen Gefährdungspotenzial verbunden.[257] Die Möglichkeit der so erhobenen Daten mit anderen Datenbeständen zu verknüpfen, um so weitere Informationen zu erlangen, birgt eine potenzielle Gefahr für die freie Entfaltung der Persönlichkeit.[258]

Ein weiteres Kriterium der Eingriffsintensität automatisierter Kfz-Kennzeichenerfassung ist dem Zweck der Maßnahme zu entnehmen. Wird diese Technik eingesetzt, um ein bestimmtes Kfz-Kennzeichen, welches zur Sachfahndung ausgeschrieben ist, zu detektieren, dann stellt dies einen relativ geringen Eingriff dar. Die Maßnahme selbst ist dann nur ein Hilfsmittel, um weitere Maßnahmen ergreifen zu können.[259] Schwerwiegender liegt der Eingriff,

---

[251] BVerwG Az. 6 C 7/13 Rn. 27.
[252] BVerfG, Urt. vom 11.03.2008 Az. 1 BvR 2074/05, 1254/07, Rn. 78.
[253] Ebd., Rn. 29.
[254] Ebd., Rn 66; Andere Auffassung: BVerwG Az. 6 C 7/13 Rn. 29.
[255] Vgl. Stettner: Sicherheit am Bahnhof, S. 119.
[256] Haberl: Automatische Kennzeichenerkennung, auf http://www.sueddeutsche.de/auto/automatische-kennzeichenerkennung-wo-ihr-nummernschild-erfasst-wird-1.2188409, abgerufen am 08.01.2018.
[257] Vgl. Stettner: Sicherheit am Bahnhof, S. 121.
[258] Vgl. ebd., S. 122.
[259] BVerfG, Urt. vom 11.03.2008 Az. 1 BvR 2074/05, 1254/07, Rn. 82.

wenn die Maßnahme eingesetzt wird, um die erhobenen Daten weiterzuverwenden und neue Informationen zu generieren. Durch das immer wieder stattfindende Detektieren bestimmter Kfz-Kennzeichen können „Informationen über das Fahr- und Bewegungsverhalten des Fahrers gewonnen werden."[260] Die Maßnahme selbst ermöglicht persönlichkeitsrelevante Informationen bzw. ein Bewegungsprofil zu erstellen und gleicht eher dem Mittel der technischen Observation. „Sie bietet dann nicht mehr lediglich einen Schlüssel zu Folgemaßnahmen, indem sie den Adressaten für diese weiteren Maßnahmen greifbar macht. Vielmehr liefert sie selbst dann schon diejenigen Informationen, auf deren Sammlung es der Polizei ankommt. Die Maßnahme effektiviert in diesem Fall nicht lediglich das bisherige Eingriffsinstrumentarium der Polizei, sondern stellt sich selbst als eine neuartige Eingriffsmöglichkeit mit potentiell hoher Persönlichkeitsrelevanz dar."[261]

2. Rechtsgrundlagen automatisierter Kfz-Kennzeichenerfassung

Die polizeiliche Maßnahme der automatisierten Kfz-Kennzeichenerfassung bedarf aufgrund ihrer Eingriffsintensität einer hinreichend bestimmten Rechtsgrundlage. Die Maßnahme selbst kann sowohl präventiven als auch einen repressiven Charakter aufweisen.[262] Repressiv ist die Maßnahme dann, wenn durch sie „Täter gefasst und weitere Stufen der Strafverfolgung realisiert werden können"[263]. Das BVerfG sieht bei einer Fahndung in einem gefilterten Datenbestand aus der INPOL-Datei „Sachfahndung" einen präventiven Zweck.[264] Das drückt sich zudem in den gesetzlich normierten Eingriffsbefugnissen der Polizeien aus.[265]

---

[260] Stettner: Sicherheit am Bahnhof, S. 123.
[261] BVerfG, Urt. vom 11.03.2008 Az. 1 BvR 2074/05, 1254/07, Rn. 90.
[262] Vgl. Kenzel: Die automatische Kennzeichenfahndung, S. 84.
[263] Stettner: Sicherheit am Bahnhof, S. 124.
[264] BVerfG, Urt. vom 11.03.2008 Az. 1 BvR 2074/05, 1254/07, Rn. 152.
[265] Der Einsatz automatische Kennzeichenerfassungsgeräte ist nicht in allen Landespolizeigesetzen normiert. Neben der Bundespolizei verfügen bspw. die Länder Bayern, Hessen, Brandenburg, Sachsen, Hamburg und Berlin über entsprechende Ermächtigungsgrundlagen.

Exemplarisch erlaubt § 27b Abs. 1 BPolG die anlassbezogene automatische Kennzeichenerfassung vorübergehend und nicht flächendeckend, „wenn

1. dies zur Abwehr einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person erforderlich ist,

2. dies auf Grund von tatsächlichen Anhaltspunkten für Straftaten von erheblicher Bedeutung, die gegen die Sicherheit der Grenze gerichtet sind, erfolgt oder

3. eine Person oder ein Fahrzeug durch die Bundespolizei oder eine andere Behörde ausgeschrieben wurde und die Begehung einer Straftat von erheblicher Bedeutung durch diese Person oder mittels des ausgeschriebenen Fahrzeugs unmittelbar bevorsteht oder andauert.“[266]

Nach Absatz 2 dürfen „die nach Absatz 1 erhobenen Daten (können) mit dem Fahndungsbestand nach § 34 Absatz 1 Satz 2 automatisch abgeglichen werden.“[267] Ähnliche Einschränkungen auf konkrete Orte und Erkenntnisse finden sich in den entsprechenden Regelungen der Landespolizeien wieder.[268] Die genauen Voraussetzungen und Modalitäten der Kennzeichenüberwachung müssten dem Bestimmtheitsgebot folgend genau geregelt sein.[269]

Die Maßnahme der automatisierten Kfz-Kennzeichenerfassung stellt zwar einen Eingriff in die Grundrechte Einzelner dar, ist aber in den einzelnen Ermächtigungsgrundlagen der Bundes- und Landespolizeien hinreichend bestimmt und verhältnismäßig.[270] Durch die Technik wird zwar eine große Bandbreite von Kfz-Kennzeichen erfasst, aber in vielen Fällen findet letztlich aufgrund der hohen Anzahl von Nicht-Treffern[271] gar kein Eingriff in das Recht auf

---

[266] Vgl. § 27b Abs. 1 BPolG.
[267] Vgl. § 27b Abs. 2 BPolG.
[268] Bspw. Art. 33 Abs. 2 Satz 2 und 3 BayPAG, Polizeiaufgabengesetz (PAG) in der Fassung der Bekanntmachung vom 14. September 1990 (GVBl. S. 397, BayRS 2012-1-1-I), das zuletzt durch § 1 des Gesetzes vom 24. Juli 2017 (GVBl. S. 388) geändert worden ist; § 8a HmbPolDVG.
[269] BVerfG, Urt. vom 11.03.2008 Az. 1 BvR 2074/05, 1254/07, Rn. 93f.
[270] BVerfG, Urt. vom 11.03.2008 Az. 1 BvR 2074/05, 1254/07.
[271] Haberl: Automatische Kennzeichenerkennung, auf http://www.sueddeutsche.de/auto/automatische-kennzeichenerkennung-wo-ihr-nummernschild-erfasst-wird-1.2188409, abgerufen am 09.01.2018.

informationelle Selbstbestimmung statt.[272] Zudem werden durch die Maßnahme alleine noch keine sensiblen Personendaten oder physiologische bzw. verhaltensbezogene Merkmale erfasst.[273]

II Mustererkennung ohne Personenbezug

Unter einer Mustererkennung ohne Personenbezug kann die Objekterkennung /-detektion verstanden werden, bei der keine personenbezogenen Daten erhoben werden.

1. Eingriffsintensität der Mustererkennung ohne Personenbezug

Für die Mustererkennung ohne Personenbezug existiert derzeit keine eigene Ermächtigungsgrundlage in den jeweiligen Polizeigesetzen. Entscheidend wäre die zu erwartende Grundrechtseinschränkung, denn bei dieser bedarf es einer Eingriffsbefugnis. Sobald personenbezogene Daten erhoben werden, liegt ein Eingriff in das Recht auf informationelle Selbstbestimmung vor. Nach dem Bundesdatenschutzgesetz sind personenbezogene Daten alle „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)“.[274] Hierunter sind Informationen über „die Person des Betroffenen oder über einen auf diesen bezogenen Sachverhalt“[275] zu verstehen.

Neben der automatisierten Kfz-Kennzeichenerfassung wurde in Kapitel C für die Objekterkennung und Detektion das Beispiel nicht zuzuordnender Gegenstände im Bereich kritischer Infrastruktur aufgeführt. Die Detektion solcher Gepäckstücke dient Informationszwecken für die Gefahrenverhütung, so dass durch diese Zweckbestimmung die Ebene der Information erreicht wird.[276] Anknüpfungspunkt ist nicht das Gepäckstück selbst, sondern die Information, dass es zurückgelassen wurde.[277] Ein Personenbezug ließe sich nur dann herstellen, wenn das Gepäckstück einer natürlichen Person zuordenbar wäre.

---

[272] Vgl. Stettner: Sicherheit am Bahnhof, S. 132.
[273] Vgl. ebd. S. 139.
[274] § 3 Abs. 1 BDSG.
[275] Stettner: Sicherheit am Bahnhof, S. 170.
[276] Dammann, in: Simitis, BDSG, § 3 Rn 5.
[277] Vgl. Stettner: Sicherheit am Bahnhof, S. 170.

Fraglich ist, ob diese Person praktisch oder absolut bestimmbar sein muss. § 3 Abs. 6 BDSG beschreibt eine Anonymisierung, wenn Gegenstände „nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können“[278] Absolut würde bedeuten, dass keine Möglichkeit mehr besteht, die Person zu bestimmen, was aufgrund getätigter Videoaufzeichnungen und durch Spuren und Informationen in und am Gepäckstück zumindest nicht gänzlich auszuschließen ist. Die Maßnahme der Gepäckdurchsuchung sowie der „Rückgriff auf Videoaufzeichnungen zur Bestimmung der Identität des Besitzers des Gepäckstücks wären ein eigenständiger Eingriff.“[279]

Für den Einsatz eines objekterkennenden und objektdetektierenden Algorithmus, der herrenlose bzw. nicht zuzuordnende Gegenstände aufmeldet, bei denen sich praktisch kein Personenbezug herstellen lässt, gilt, dass kein Eingriff in das Recht auf informationelle Selbstbestimmung vorliegt.[280] Anders gestaltet sich der Fall bei einem Personentracking, selbst wenn man bei diesem keine physiologischen bzw. verhaltensbezogene Merkmale erfasst werden, sondern lediglich softbiometrischer Merkmale, wie Kleidung. Hier bezieht sich der Informationszweck auf eine Person und ist zugleich personenbezogen.[281]

2. Rechtsgrundlage der Mustererkennung ohne Personenbezug

Im Falle der Mustererkennung ohne Personenbezug wäre keine eigenständige Eingriffsbefugnis notwendig, da in kein Grundrecht eines Betroffenen eingegriffen wird. Bei dieser Technikanwendung ohne Personenbezug bleibt es aber auch bei einem eingeschränkten kriminalistischen Nutzen. Damit diese Technologie eine präventive und repressive Wirksamkeit entfalten kann ist der Bezug zu potenziellen Tätern notwendig. Dies würde dann aber unter den Bereich Mustererkennung mit Personenbezug fallen.

---

[278] § 3 Abs. 6 BDSG
[279] Stettner: Sicherheit am Bahnhof, S. 171.
[280] Vgl. ebd. S. 171.
[281] Dammann, in: Simitis, BDSG, § 3 Rn 5.

III Mustererkennung mit Personenbezug

Die technischen Einsatzmöglichkeiten intelligenter Systeme mit Personenbezug sind, wie in den Kapiteln C und D dargestellt, vielfältig. Als wesentliche Analyseobjekte der Mustererkennung in der Sicherheitstechnologie ist die biometrische Erkennung mit ihren physiologischen bzw. verhaltensbezogenen Merkmalen zu nennen. Die Streubreite von Gesichtserkennung über Verhaltensanalyse bis hin zum Personentracking erfordert eine getrennte Betrachtung der einzelnen Merkmale, ohne dabei das Zusammenspiel der Anwendungen zu vernachlässigen.[282]

1. Eingriffsintensität der Mustererkennung mit Personenbezug

Als Maßstab jeder rechtlichen Prüfung über die Legitimation einer polizeilichen Eingriffsbefugnis steht die Menschenwürde gem. Art. 1 Abs. 1 GG. Eine Technik, die das Potenzial hat, selbstständig, schnell und effektiv eine Vielzahl von Menschen zu überwachen, birgt die Gefahr, dass Menschen verdinglicht werden und VÜ zu einem totalen Überwachungsstaat beiträgt. Die Algorithmen haben die Aufgabe, Situationen noch vor einem menschlichen Entscheider einzuschätzen und Entscheidungen zu treffen. Dies birgt Gefahren für die Menschenwürde und stellt den Einsatz dieser Technologie in Frage. Ein weiterer zentraler Maßstab stellt das Recht auf informationelle Selbstbestimmung und die Gleichheitsgrundrechte dar.

a) Die Menschenwürde

Durch den Einsatz intelligenter Systeme der VÜ könnte ein Eingriff in die Würde des Menschen vorliegen. Das Bundesverfassungsgericht zählt als mögliche Verletzungshandlungen die „Erniedrigung, Brandmarkung, Verfolgung und Ächtung“[283], die zu einem Absprechen des Achtungsanspruchs des Individuums führen kann.[284] Die Objektformel schützt den Einzelnen davor, zum bloßen Objekt staatlichen Handelns herabgewürdigt zu werden.[285] Neben der Objektformel führt *Held* weitere Ansätze wie beispielsweise die Leistungs-

---

[282] Vgl. Held: Intelligente Videoüberwachung, S. 71.
[283] BVerfG Entscheidung 1, 97, 104.
[284] Vgl. Stettner: Sicherheit am Bahnhof, S. 141.
[285] Vgl. Herdegen in: Maunz/Dürig: Grundgesetz, Art. 1 Abs. 1 GG, Rn. 36.

oder die Kommunikationstheorie zum Stand und zur Bestimmung der Würdediskussion an.[286]

Zu prüfen ist, ob durch die Datenerhebung oder die erhobenen Daten selbst eine Verletzung der Menschenwürde gegeben ist. Durch das Erstellen eines Template auf Grundlage biometrischer Vermessung des Gesichts eines Individuums, „sogar ohne Wissen und Zutun der betroffenen Person“[287], könnte diese zum Objekt herabgewürdigt werden. Der Begriff der Menschenwürde ist eng auszulegen, um das hohe Schutzgut nicht herabzuwürdigen.[288] Weiterhin müssten die erhobenen Daten eine Verletzung der Intimsphäre darstellen. Durch das Videografieren und Feststellen äußerlicher Merkmale und sonstiger Messungen liegt „kein physisches Eindringen in die Intimsphäre durch einen Polizeibeamten“[289] vor. Der Einsatz von technischen Mitteln zur Erfassung offener Merkmale, die jedem ersichtlich sind, stellt keine Objektivierung des Individuums dar.[290] Sie sind Teil erkennungsdienstlicher Maßnahmen, die sowohl im präventiven Polizeirecht,[291] als auch in der Strafprozessordnung[292] normiert sind und keinen Verstoß gegen die Menschwürde darstellen. Stettner kommt zu dem Entschluss, dass der Zweck der Gesichtserkennung die Identifizierung der Person ist und „hierdurch wird der Betroffene als Subjekt mit einer eigenen Individualität anerkannt, so dass von keiner Verobjektivierung gesprochen werden kann.“[293] Die Gesichtserkennung ist nicht von vornherein entwürdigend,[294] unterliegt aber einer engen „Ausgestaltung der Einsatzintensitäten und -modalitäten“.[295]

---

[286] Vgl. Held: Intelligente Videoüberwachung, S. 66ff.
[287] Stettner: Sicherheit am Bahnhof, S. 142.
[288] Vgl. ebd., S. 144.
[289] Ebd., S. 144.
[290] Vgl. ebd., S. 144f, Held: Intelligente Videoüberwachung, S. 143.
[291] Vgl. § 24 Abs. 3 BPolG, Art. 14 BayPAG, § 14 PolG NRW.
[292] Vgl. § 81b StPO.
[293] Stettner: Sicherheit am Bahnhof, S. 145.
[294] Andere Auffassung vertritt Müller. Er sieht in einer biometrischen Erfassung bereits einen entwürdigenden Eingriff. Vgl. Müller: Videoüberwachung in öffentlich zugänglichen Räumen, S. 102.
[295] Held: Intelligente Videoüberwachung, S. 77.

Auch der Einsatz von Algorithmen zur Verhaltenserkennung könnte einen Eingriff in die Würde des Menschen begründen. Mit der automatisierten Verhaltensanalyse sollen Überschreitungen von zuvor festgelegten Grenzen gemeldet werden. Sie trifft nur eine Vorauswahl, in dem sie ein bestimmtes Verhalten oder Muster erkennt. Dies entfaltet für den Betroffenen keine direkten Auswirkungen.[296] Im Falle eines Treffers würde sich ein menschlicher Operator einschalten und die Situation beobachten und weitere Maßnahmen veranlassen. Insgesamt kann davon ausgegangen werden, dass der Eingriff so gering ist, dass nicht von einer „Würdegefährdung“[297] gesprochen werden kann.[298]

Kritiker führen an, dass die Verhaltensanalyse mittels VÜ zur Erstellung von Persönlichkeitsprofilen genutzt werden könnte.[299] Wäre es durch den Einsatz der technischen Verhaltensanalyse möglich, von konkreten Verhaltensweisen einen Rückschluss auf die Gedanken, Gefühle und die Persönlichkeit zu schließen, so würde ihr Einsatz gegen die Würde verstoßen.[300] Dem ist entgegenzuhalten, dass lediglich äußere Verhaltensweisen und Körperfunktionen beobachtet und analysiert werden und dass sich dadurch kein Rückschluss auf die psychischen Zustände des Betroffenen ergeben. Somit lässt sich auch kein Persönlichkeitsprofil eines Individuums anlegen.[301] Eine Verletzung der Menschenwürde durch den Einsatz der VÜ zur Verhaltensanalyse ist daher im Regelfall zu verneinen.

Das Personentracking ist eine kombinierte technische Maßnahme aus der Gesichtserkennung und der Verhaltensanalyse, die die Verfolgung einer sich durch den Raum bewegenden Person ermöglicht. Auch wenn beide Maßnahmen vereint einen tieferen Eingriff in Grundrechte eines Betroffenen darstellen können, so sind diese nicht per se entwürdigend. Entscheidend sind neben der Dauer und Wiederholung der Maßnahme gegenüber dem Einzelnen auch

---

[296] Vgl. Held: Intelligente Videoüberwachung, S. 74; vgl. Stettner: Sicherheit am Bahnhof, S. 154.
[297] Held: Intelligente Videoüberwachung, S. 74.
[298] Vgl. Stettner: Sicherheit am Bahnhof, S. 154.
[299] Vgl. Büllesfeld: Polizeiliche Videoüberwachung, S. 16.
[300] BGH, Urteil vom 17.12.1998 Az. 1 StR 156/98, Rn. 28; vgl. Held: Intelligente Videoüberwachung, S. 74; Stettner: Sicherheit am Bahnhof, S. 155.
[301] Vgl. Held: Intelligente Videoüberwachung, S. 74; vgl. Stettner: Sicherheit am Bahnhof, S. 155f.

die Zielsetzung und die konkreten Umstände des Einzelfalls.[302] Eine Entwürdigung kann beispielsweise durch eine permanente Verfolgung einer Person gegeben sein. Dies widerspreche aber den technischen Möglichkeiten und vorgestellten Einsatzszenarien.

Durch den Einsatz intelligenter Systeme der VÜ durch Mustererkennung mit Personenbezug wird das hohe Gut der menschlichen Würde grundsätzlich nicht verletzt. Jedoch besteht die latente Gefahr, dass durch einen ausufernden Einsatz bzw. durch die Verknüpfung mit weiteren Systemen und Datenbanken die Individualität des Einzelnen verloren geht oder die Eingriffsintensität zu groß wird.[303]

b) Das Recht auf informationelle Selbstbestimmung

Da es bei der Mustererkennung mit Personenbezug insbesondere auf Personen als Ziel einer Analyse (hierbei ist es unerheblich, welche der drei Verfahren angewandt wird) ankommt, ist einen Personenbezug immer gegeben. Zum Schutzgut des Betroffenen gehören auch das Verhalten und die äußeren Erscheinungsmerkmale.[304] Sobald ein menschlicher Entscheider aufgemeldete Daten sichtet und prüft, ist ein Personenbezug gegeben und das Recht auf informelle Selbstbestimmung tangiert.[305] Hierbei ist es unerheblich, ob ein realer Treffer oder ein Fehlalarm vorliegt. Anknüpfungspunkt ist das Verlassen der Information aus dem geschlossen Computersystem und das Zugänglichwerden eines Personenbezugs gegenüber einem menschlichen Entscheider.[306] Im Falle der Gesichtserkennung liegt eine Verletzung bereits bei der Erhebung von Rohdaten einer Person von. Ein zweiter Eingriff erfolgt dann durch die Erstellung von Templates, da diese, selbst wenn sie verschlüsselt wären, immer noch aus individuell zuordenbaren Daten bestehen und so einen Personenbezug deklarieren.[307] Lediglich bei einem Nicht-Treffer, bei dem die

---

[302] Vgl. Held: Intelligente Videoüberwachung, S. 75.
[303] Vgl. ebd., S. 74; Stettner: Sicherheit am Bahnhof, S. 155f.
[304] Vgl. Stettner: Sicherheit am Bahnhof, S. 157; vgl. Hornung/Desoi: "Smart Cameras" und automatische Verhaltensanalyse, S. 153.
[305] Vgl. Held: Intelligente Videoüberwachung, S. 109; vgl. Stettner: Sicherheit am Bahnhof, S. 157.
[306] Vgl. Stettner: Sicherheit am Bahnhof, S. 157.
[307] Vgl. ebd., S. 146.

Daten anonym bleiben und sofort gelöscht werden, so dass kein Zugriff außerhalb des Computersystems möglich ist, findet kein Eingriff in das Recht auf informelle Selbstbestimmung statt.[308]

c) Das allgemeine Persönlichkeitsrecht

Held ging der Frage nach, ob durch das Recht auf informationelle Selbstbestimmung ein generell subjektiv-rechtlicher Schutz vor Einschüchterungseffekten vorliegt. Er kam zu dem Ergebnis, dass dem nicht so sei und dass dieser Schutz sich „teilweise, wohl als subsidiärer Schutz, in Art. 2 Abs. 1 GG verorten“[309] lässt bzw. weitere spezielle Grundrechte in ihrem Schutzbereich tangiert sind.[310] Neben der besonderen Ausprägung des Persönlichkeitsrechts im Recht auf informationelle Selbstbestimmung könnte also auch das allgemeinen Persönlichkeitsrecht tangiert werden. Dies wäre dann gegeben, wenn durch den Einsatz intelligenter VÜ Einschüchterungseffekte ausgehen. Neue Technologien, insbesondere solche, die der Überwachung dienen, können bei den Nutzern der überwachten Räume zu Unbehagen führen. Zum einen fehlt es den Betroffenen an Wissen über die Arbeitsweise der Algorithmen und zum anderen ist für sie nicht immer ersichtlich, durch welche Verhaltensweisen ein Alarm ausgelöst wird. Diese Unwissen- und Unsicherheit können Einfluss auf den Einschüchterungseffekt haben.[311]

d) Die Gleichheitsgrundrechte

Die Gleichheitsgrundsätze schützen vor Verletzungen einer Ungleichbehandlung von Gleichem und einer Gleichbehandlung von Ungleichem und dadurch unmittelbar vor Diskriminierung.[312] Algorithmen arbeiten zwar auf Grundlage von Statistiken und Wahrscheinlichkeiten, dennoch kann es hierbei zu Ungleichbehandlungen kommen. Bei der Mustererkennung mit Personenbezug können besondere Merkmale, wie das Aussehen und das Verhalten erkannt werden, da es gerade auf diese ankommt.[313] Entscheidend ist, dass dieses Merkmal nicht zu einer Benachteiligung führen darf. Deshalb darf der gesetzte

---

[308] Vgl. Stettner: Sicherheit am Bahnhof, S. 156.
[309] Vgl. Held: Intelligente Videoüberwachung, S. 89.
[310] Vgl. ebd. S. 87.
[311] Vgl. ebd. S. 87f; vgl. Stettner: Sicherheit am Bahnhof, S. 156.
[312] Vgl. Stettner: Sicherheit am Bahnhof, S. 161.
[313] Vgl. ebd. S. 167.

Rahmen der zu detektieren Merkmale nicht unendlich weit gefasst sein (nur Hautfarbe, Rasse, etc.), sondern muss so eng sein, dass er geeignet ist, eine gegenwärtige, konkrete Gefahr zu beseitigen.[314] Problematisch könnten demnach Konstellationen werden, bei denen ein Merkmal zur Identifizierung eines Einzelnen eine ganze Gruppe von Merkmalsträgern als Detektionsziel deklariert.[315] *Held* sieht zudem nur einen sehr kurzen Zeitraum als legitim an, um keine stigmatisierende Wirkung durch den Einsatz dieser Technik aufkommen zulassen.[316] Gleichzeitig sieht er auch Vorteile gegen eine Ungleichbehandlung durch den Einsatz dieser Technik, da Algorithmen im Vergleich zum Menschen wertfrei und neutral arbeiten. Er beschreibt das Verhältnis von intelligenter VÜ und den Gleichheitsgrundrechten zwischen „Relevanz und Relativität".[317]

e) Fazit

Der Einsatz von intelligenter VÜ mit Personenbezug greift in die Grundrechte der überwachten Personen ein. Eine grundlegende Verletzung der Menschenwürde wäre unter den in Kapitel D skizzierten Einsatzszenarien nicht gegeben. Da es bei diesen Verfahren immer auf einen Personenbezug ankommt, ist das Recht auf informationelle Selbstbestimmung immer dann tangiert, wenn eine Treffermeldung das geschlossen Computersystem verlässt und dadurch eine Information nicht mehr nur kurzfristig und anonym ist. Weiterhin können durch Einschüchterungseffekte das allgemeine Persönlichkeitsrecht und weitere spezielle Grundrechte tangiert werden. Je nach Einsatzgebiet und Anwendung im konkreten Einzelfall können zudem die Gleichheitsgrundrechte verletzt werden. Grundsätzlich birgt die Technologie die Gefahr, dass durch einen flächendeckenden, tiefgreifenden oder in Kombination durch den Einsatz verschiedener Module ein kritisches Niveau erreicht wird. Insbesondere „die Eingriffskriterien Streubreite und Massenhaftigkeit werden für die Überprüfung intelligenter Videoüberwachung relevant."[318]

---

[314] Vgl. Held: Intelligente Videoüberwachung, S. 174; vgl. Stettner: Sicherheit am Bahnhof, S. 169.
[315] Vgl. ebd. S. 219.
[316] Vgl. Held: Intelligente Videoüberwachung, S. 174.
[317] Ebd. S. 175.
[318] Ebd. S. 218.

2. Anforderung an mögliche Rechtsgrundlagen der Mustererkennung mit Personenbezug

Für den polizeilichen Einsatz von VÜ öffentlich zugänglicher Räume unter Berücksichtigung „intelligenter“ Systeme durch Mustererkennung mit Personenbezug besteht derzeit keine Ermächtigungsgrundlage, die den Einsatz ausdrücklich normiert.[319] *Held* und *Stettner* sind der Frage nachgegangen, ob der Einsatz intelligenter Videoüberwachungssysteme durch derzeit bestehendes Recht legitimiert sein könnte.[320] Als mögliche Ermächtigungsrundlagen kamen aufgrund der Ähnlichkeit der Maßnahmen die Identitätsfeststellung, der Einsatz konventioneller VÜ und die Rasterfahndung in Betracht.[321] Beide kommen zu der Auffassung, dass der Begriff intelligente VÜ ein Synonym für „ein sehr flexibles Instrument ist, das in unterschiedlichen Szenarien zu verschiedenen taktischen Zwecken eingesetzt werden kann“[322] und dadurch eine hohe Eingriffsintensität vorliegt, denen man nur mit spezifischen Rechtsgrundlagen begegnen kann.[323]

Als materielle Voraussetzung zur Schaffung einer neuen Norm muss der Verhältnismäßigkeitsgrundsatz gewahrt werden. Intelligente Videoüberwachungssysteme würden persönlichkeitsrelevante Daten erfassen, mit Datenbeständen abgleichen und durch ihre große Streubreite einen intensiven Eingriff[324], vergleichbar mit der präventiven Rasterfahndung, darstellen.[325] Die hohe Eingriffsintensität macht es notwendig, dass für den Einsatz einer solchen Technik grundsätzlich eine konkrete Gefahr[326] vorliegen muss. Hiervon kann der Gesetzgeber aber abweichen, um auf geänderte Bedrohungslagen

---

[319] Vgl. Stettner: Sicherheit am Bahnhof, S. 171; vgl. Held: Intelligente Videoüberwachung, S. 188.
[320] Vgl. ebd., S. 171; vgl. Held: Intelligente Videoüberwachung, S. 176f.
[321] Vgl. ebd. S. 171.
[322] Held: Intelligente Videoüberwachung, S. 199.
[323] Vgl. Stettner: Sicherheit am Bahnhof, S. 177.
[324] BVerfG, Beschluss vom 04.04.2006 Az. 1 BvR 518/02, Rn. 141.
[325] Vgl. Stettner: Sicherheit am Bahnhof, S. 178.
[326] Anmerkung des Verfassers: Die Gefahr ist dann konkret, wenn im entsprechenden Einzelfall bzw. nach der Lebenserfahrung ein sofortiger Handlungsbedarf besteht, mit hinreichender Wahrscheinlichkeit in naher Zukunft mit einem Schadenseintritt zu rechnen ist, vgl. Möllers: Wörterbuch der Polizei, Gefahr, S. 762.

reagieren zu können.[327] Hierbei muss das Verhältnis zwischen Eingriffsintensität und Eingriffsvoraussetzungen gewahrt bleiben.[328] Denkbar wäre ein Einsatz im Gefahrenvorfeld an gefährdeten Orten zum Schutz hochrangiger Rechtsgüter[329] oder zur Verhinderung schwerer Straftaten[330]. So soll verhindert werden, dass eine Maßnahme mit einer hohen Eingriffsintensität zu einem Bekämpfungsmittel von Alltagsdelikten degradiert wird.[331]

Obwohl eine derartige Maßnahme hinreichend bestimmt sein muss, sollte aus polizeitaktischen Erwägungen und dem fortwährenden technischen Fortschritt eine gewisse Offenheit in den Formulierungen der Ermächtigungsgrundlagen gewahrt bleiben. Diese könnte durch einen eingeräumten Ermessenspielraum der Polizeibehörden bei dem *Ob* und dem *Wie* des Einsatzes einer solchen intelligenten VÜ umgesetzt werden.[332] Zudem muss der Einsatz den datenschutzrechtlichen Bestimmungen gerecht werden. Insbesondere die analogen Anwendungen aus den Regelungen der konventionellen VÜ zu den Löschfristen und Hinweispflichten, aber auch dem Prinzip der Datenvermeidung durch eine Verringerung von Erhebungen individueller Daten muss Anwendung finden. Durch das Erfüllen der Hinweispflicht, durch explizite Hinweise auf den Einsatz entsprechender Systeme[333] würde die Maßnahme offen durchgeführt und so einer eingriffsintensivierenden heimlichen/ verdeckten VÜ entgegenwirken. Mögliche Formulierungen könnten wie folgt aussehen:

„Für Ihre Sicherheit und zum Schutz hochrangiger Rechtsgüter wird dieser Bereich mit Gesichtserkennung videoüberwacht“

bzw.

---

[327] Vgl. Stettner: Sicherheit am Bahnhof, S. 179.
[328] Vgl. ebd. S. 179.
[329] BVerfG, Beschluss vom 04.04.2006 Az. 1 BvR 518/02, Rn. 1.
[330] Analog dem Straftatenkatalog, gem. § 100a Abs. 2 Nr. 1 StPO (Telekommunikationsüberwachung).
[331] Vgl. Stettner: Sicherheit am Bahnhof, S. 181.
[332] Vgl. Stettner: Sicherheit am Bahnhof, S. 181; vgl. Held: Intelligente Videoüberwachung, S. 201.
[333] Andere Auffassungen hierzu vertreten Gaul: Untersuchung der verfassungsrechtlichen Anforderungen an Videoüberwachungsmaßnahmen des Staates im öffentlichen Raum mit und ohne biometrische Erkennungsverfahren unter besonderer Berücksichtigung der hermeneutischen Erkenntnismethoden im Verfassungsrecht, S. 119 sowie Held: Intelligente Videoüberwachung, S. 135.

„Für Ihre Sicherheit und zum Schutz hochrangiger Rechtsgüter wird dieser Bereich mit Verhaltenserkennung videoüberwacht“

oder auch

„Für Ihre Sicherheit wird dieser Bereich videoüberwacht und die erhobenen Daten automatisiert ausgewertet“

Der Hinweis kann auch aus Kombinationen einzelner Maßnahmen bestehen, er sollte aber vollumfänglich auf alle Bestandteile, sowie dem Ziel der Maßnahme hinweisen.[334]

Wichtig wäre dabei, die Maßnahme konkret zu benennen, um durch Transparenz Akzeptanz zu schaffen[335] und dem Einschüchterungseffekt durch die Unwissenheit der Betroffenen entgegenzuwirken. Der Einsatz einer solchen Technik würde dann auch nicht unter einem Richtervorbehalt stehen, sondern könnte durch einen Behördenleiter angeordnet werden.[336] Zudem sprechen sich beide Autoren für eine Evaluationspflicht und Beteiligung des Datenschutzbeauftragten aus.[337] *Held* und *Stettner* implizierten die Maßnahme der intelligenten VÜ in Form einer automatisierten Auswertung bzw. dem Abgleich biometrischer Daten unter den oben genannten Anforderungen im Art. 32 PAG zur Datenerhebung bei öffentlichen Veranstaltungen und Ansammlungen sowie an besonders gefährdeten Objekten.[338]

Neben den Möglichkeiten zum Einsatz von Mustererkennung mit Personenbezug zur Gefahrenabwehr wurde in Kapitel D Einsatzszenarien einer intelligenten VÜ vorgestellt, die als Instrument der Repression angesehen werden können. Ihr Schwerpunkt liegt in der strafrechtlichen Analyse und Auswertung von Videoaufzeichnungen. Die Eingriffsintensität wäre in einer retrograden Videoanalyse vergleichbar derer einer Echtzeitanalyse. Wenn die Zielsetzung aber nicht mehr dem Gefahrenabwehrrecht, sondern der Strafverfolgung zuzuord-

---

[334] Vgl. Held: Intelligente Videoüberwachung, Vorschlag zu Art. 32 Abs. 2 Satz 3 PAG, S. 202.
[335] Vgl. Stettner: Sicherheit am Bahnhof, S. 182.
[336] Vgl. ebd. S. 183; vgl. Held: Intelligente Videoüberwachung, S. 201.
[337] Vgl. ebd. S. 184; vgl. Held: Intelligente Videoüberwachung, S. 201.
[338] Vgl. ebd. S. 185f; vgl. Held: Intelligente Videoüberwachung, S. 202f.

nen ist, dann wäre eine etwaige Ermächtigungsgrundlage in der Strafprozessordnung zu verorten. Die bestehende Eingriffsgrundlage des § 81b StPO ermächtig nicht die Erhebung und den Abgleich eines biometrischen Datensatzes.[339] Aufgrund der Eingriffsintensität etwaiger Maßnahmen könnte der § 131b StPO (Veröffentlichung von Abbildungen des Beschuldigten oder Zeugen) zur Bestimmung der Voraussetzung Anwendung finden. Hiernach muss der Beschuldigte einer Straftat von erheblicher Bedeutung verdächtig sein, denn die tatbestandliche Voraussetzung einer Straftat bringt das Übermaßverbot zum Ausdruck und stellt klar, dass eine Öffentlichkeitsfahndung bei geringfügigen Straftaten untersagt ist.[340]

IV Akzeptanz von VÜ öffentlich zugänglicher Räume unter Berücksichtigung „intelligenter“ Systeme

Für den legitimen Einsatz von „intelligenter“ Videoüberwachungstechnik öffentlich zugänglicher Räume bedarf es neben entsprechender Rechtsgrundlagen auch der Akzeptanz der Bevölkerung. Diese könnte per lege unterstellt werden, wenn entsprechende Ermächtigungsgrundlagen durch Gesetzgebungsverfahren bestehen würden. Die Effektivität der VÜ steht aber auch in Abhängigkeit zu der Reaktion der Bevölkerung auf diese Technik, daher ist über die gesetzliche Legitimation hinaus der Zuspruch der breiten Öffentlichkeit zur Gewährleistung der Wirksamkeit notwendig.

Verschiedene empirische Studien zeigen, dass die konventionelle VÜ in Deutschland eine hohe Zustimmung in der Bevölkerung erfährt und das obwohl das subjektive Sicherheitsgefühl nicht relevant gesteigert wird.[341] Die Zustimmungsquoten schwanken zwischen 50 und 90 %[342] und stehen in Abhängigkeit zu weiteren polizeilichen Maßnahmen und begleitender Öffentlichkeitsarbeit.[343] Die Akzeptanz konventioneller VÜ beruht aber nicht auf einem unerschütterlichen Technikglauben, sondern eher auf einer „besser als gar nichts“

---

[339] Vgl. Herrmann: Möglichkeiten und Grenzen des Einsatzes biometrischer Verfahren, S. 167.
[340] AG Hannover, 23.04.2015 - 174 Geschäftszeichen 434/15, Rn. 6.
[341] Vgl. Kudlacek: Akzeptanz von Videoüberwachung, S. 145; vgl. Apelt/Möllers: Wie „intelligente“ Videoüberwachung erforschen?, S. 586.
[342] Vgl. Apelt/Möllers: Wie „intelligente“ Videoüberwachung erforschen?, S. 587.
[343] Vgl. Dietrich: Wirksamkeit der polizeilichen Videoüberwachung, S. 58.

Einstellung der Befragten.[344] *Zurawski* konnte in einem Forschungsprojekt zwischen 2003-2006 den komplexen Zusammenhang zwischen individueller Raumwahrnehmung, öffentlichem Diskurs, Sicherheitsgefühl und der Bewertung der VÜ ableiten.[345] Er ermittelte ein positiv verzerrtes Bild der Bevölkerungsmeinung, da viele den Einsatz einer solchen Technik nicht richtig reflektierten und sich selbst gar nicht als Betroffene der Maßnahme sahen.[346] *Apelt/Möllers* kommen zu der Auffassung, dass „der öffentliche Diskurs sowohl die Akzeptanz von Sicherheitsmaßnahmen als auch das subjektive Sicherheitsgefühl – diese aber auf jeweils sehr unterschiedliche Weise – beeinflusst“[347] werden. Die Einstellung der Bevölkerung gegenüber der Technik bestimmt zudem maßgeblich die präventive und repressive Wirkung der VÜ.[348]

Für die Etablierung intelligenter Systeme der VÜ bedeutet dies, dass neben einer legitimierten Rechtsgrundlage auch die Akzeptanz der Bevölkerung eine Rolle spielt, damit die neue Technologie zur Verbesserung der Kriminalprävention und -repression beitragen kann. Gelingen kann das mit einer begleitenden Öffentlichkeitsarbeit, die Transparenz über die Einsatzmöglichkeiten und Einsatzerfolge schafft und dabei ein besonderes Augenmerk auf die datenschutzrechtlichen Verbesserungen legt. Nicht außer Acht gelassen werden dürfen Nebeneffekte, wie die räumliche Verdrängung, Unsicherheitsgefühle und Einschüchterungseffekte, die durch den Einsatz intelligenter Systeme zunehmen könnten und somit auch die Akzeptanz der breiten Bevölkerung schmälern würden.

V Zusammenfassung

Die technische Weiterentwicklung der VÜ im Bereich der Mustererkennung ermöglicht neue Möglichkeiten der Kriminalprävention und der Strafverfolgung, wirft aber auch neue rechtliche Fragen auf. Einige Einsatzszenarien, wie die automatisierte Kfz-Kennzeichenerfassung und die Mustererkennung ohne Personenbezug, kann das geltende Recht angemessen verarbeiten.[349] Bei

---

[344] Vgl. Dietrich: Wirksamkeit der polizeilichen Videoüberwachung, S. 59.
[345] Vgl. Zurawski: Videoüberwachung in Medien – Macht – Demokratie, S. 8.
[346] Vgl. Dietrich: Wirksamkeit der polizeilichen Videoüberwachung, S. 59.
[347] Apelt/Möllers: Wie „intelligente“ Videoüberwachung erforschen?, S. 588.
[348] Vgl. Dietrich: Wirksamkeit der polizeilichen Videoüberwachung, S. 66.
[349] Vgl. Hornung/Schindler: Das biometrische Auge der Polizei, S. 209.

wesentlichen Änderungen, die mehr als ein „gradueller Entwicklungsschritt einzustufen“[350] sind, bedarf es der Entscheidung des demokratischen Gesetzgebers. Zuvor ist, schon aus verfassungsrechtlicher Sicht, eine „sorgfältige Analyse der tatsächlichen Wirksamkeit zur Kriminalitätsbekämpfung“[351] nötig. Sollte die neue Technologie eine gesetzliche Legitimation erhalten, so ist auch bei deren Einsatz auf eine grundrechtsschonende Umsetzung zu achten, um Szenarien der Massenüberwachung vorzubeugen.[352]

Die große Stärke der intelligente VÜ liegt darin, dass sie sowohl freiheitsschützend als auch freiheitsgefährdend ist. Freiheitsschützend ist sie im Vergleich zur konventionellen VÜ, da der Einzelne weniger in das Blickfeld der Polizei gelangt. Durch die Sondierung durch einen Algorithmus werden nur Situationen aufgeschaltet, die vorher als wichtig definiert wurden. Die große Mehrheit der Nutzer im videoüberwachten Raum kann sich so bedenkenlos bewegen, ohne dass sie „aufgeschaltet“ werden. So kann ein technischer Grundrechtsschutz gewährleistet werden, da nur Daten bereitgestellt werden, wenn sie von „sicherheitsrechtlicher Relevanz sind, während andernfalls die fraglichen Daten automatisch gelöscht werden, ohne dass diese Dritten zur Kenntnis gebracht werden.“[353] *Roßnagel, Desoi* und *Hornung* führen beispielsweise ein Drei-Stufen-Modell als Vorschlag zur grundrechtsschonenden Gestaltung an, mit Hilfe derer eine verhältnismäßige intelligente Videoüberwachung realisierbar wäre.[354] Diese ist auch notwendig, um die Akzeptanz der Bevölkerung über die gesetzliche Legitimation hinaus zu wahren, da die Effektivität der intelligenten VÜ ebenso wie die konventionelle VÜ in Abhängigkeit zu der Reaktion der Bevölkerung gegenüber dieser Technik steht.

---

[350] Held: Intelligente Videoüberwachung, S. 48.
[351] Vgl. Hornung/Schindler: Das biometrische Auge der Polizei, S. 209.
[352] Vgl. ebd. S. 209.
[353] Würtenberger: Rechtswissenschaftliche Begleitforschung zur intelligenten Videoüberwachung, S. 4; vgl. Bergfink: Videoüberwachung im öffentlichen Personennahverkehr, S. 41f
[354] Vgl. Roßnagel/Desoi/Hornung: Gestufte Kontrolle bei Videoüberwachungsanlagen, S. 694f; Kritsch dazu Held: Intelligente Videoüberwachung, S. 154.

G Mögliche Risiken des Einsatzes von polizeilicher VÜ öffentlich zugänglicher Räume unter Berücksichtigung „intelligenter“ Systeme

Mit der Etablierung neuer kriminalistischer Techniken und Verfahren sind neben Chancen auch immer Risiken verbunden. Diese können sich individuell auf Betroffene auswirken, aber auch zu gesamtgesellschaftlichen Folgen führen und natürlich Auswirkungen auf die agierenden Nutzer haben. Einige Risiken sind gewollt oder werden zumindest geduldet und andere können ein solches Ausmaß und Unkalkulierbarkeit annehmen, welche die gesamten Maßnahmen in Frage stellen. Kritiker zeichnen ein Bild der totalen Überwachung eines an Foucaults angelehnten „algorithmisches Panopticon.“[355]

I Risiken für Nutzer videoüberwachter Räume

Die präventive VÜ zielt, durch ein „Gefühl des Beobachtetwerdens“[356] bewusst auf eine Verhaltensänderung bei den Nutzern der überwachten Räume ab. So sollen potenzielle Täter abgeschreckt und potenzielle Opfer durch die Kameras sensibilisiert werden. Neben diesen gewollten Verhaltensänderungen (Abschreckungseffekt) können aber ebenso ungewünschte Nebeneffekte durch Einschüchterung auftreten.[357] *Koch, Held u.a.* konnten feststellen, dass sich Personen tendenziell beeinträchtigter fühlten, wenn sie erfuhren, dass sie durch iVÜ überwacht werden, als Personen, die konventioneller VÜ ausgesetzt waren. Zudem stellten sie fest, dass der „subjektiv erlebte Stress zu Beginn der Überwachung in Verbindung mit Informationen zu intelligenter Technik“[358] auftrat bzw. verstärkt wurde, im Vergleich zur konventionellen VÜ. Nach der Theorie der objektiven Selbstaufmerksamkeit nimmt sich der Beobachtete selbst als Objekt wahr und versucht sein Verhalten den Standards seiner Umwelt anzupassen, um nicht aufzufallen.[359] Dieser Effekt dürfte sich verstärken, wenn Bereiche durch Systeme überwacht werden, die unangepasstes Verhalten erkennen sollen. Auch wenn die Arbeitsweise eines solchen Algorithmus nicht transparent ist, so wird der Nutzer des überwachten Raumes sein Verhalten dahingehend versuchen anzupassen, dass er nicht auffällt oder er wird

---

[355] Kees: Algorithmisches Panopticon, S. 30.
[356] Vgl. Stettner: Sicherheit am Bahnhof, S. 72.
[357] Vgl. ebd., S. 72; Dem widersprechend: vgl. Stolle: Situative Kriminalprävention, S. 229.
[358] Koch/Held u.a.: Intelligente Videoüberwachung: eine Handreichung, S. 19.
[359] Vgl. Dolderer: Verfassungsfragen der „Sicherheit durch Null-Toleranz”, S. 131.

den überwachten Raum, soweit es ihm möglich ist, meiden. Zu diesem Ergebnis kommen auch *Koch, Held u.a*. in ihrer Studie.[360] Gleichwohl stellen sie fest, dass es keine Forschung gibt, die speziell diesen Einschüchterungseffekt von Videoüberwachung untersucht. Vielmehr lässt sich vermuten, dass die „reine Überwachungssituation für eine Einschüchterung nicht ausreicht und […] dass andere Faktoren, bspw. das Aufzeigen möglicher Konsequenzen, eine Einschüchterung bedingen können."[361]

Sie stellen weiterhin fest, dass bereits nach kurzer Zeit eine Gewöhnung an die neuen Methoden der VÜ stattfindet und schließen daher nicht aus, dass die Unsicherheiten auftreten, weil die neue Technik und ihre Wirkungsweise noch unbekannt ist.[362] Durch die Anpassung des Einzelnen, um staatlichen Sanktionen zu entgehen, entsteht eine selbstdisziplinierende Wirkung und Konformität, die sich in konkreter Ausprägung selbst bei einem Nicht-Betroffenen im sog. „chilling-effect" [363] ausdrückt. Dieser beschreibt eine latente Angst, dass der Staat, obwohl kein Fehlverhalten vorliegt, Daten erhebt und speichert.[364] Dem entgegenzuwirken, sollte wie in Kapitel F beschrieben, bei einer intelligenten VÜ eine hohe Eingriffsschwelle bei gleichzeitiger Löschpflicht bei fehlender Übereinstimmung und einer begrenzten Aufbewahrungsdauer bei einem Treffer definiert werden. Zudem besteht die Gefahr, dass aus den gewonnen Bilddaten von Personen weitere Informationen abgelesen werden oder durch andere Datenbanken abgerufen werden.[365]

Die beschriebenen Effekte wirken sich in erster Linie auf die Individuen und langfristig auch auf die Gesellschaft aus.[366]

---

[360] Vgl. Koch/Held u.a.: Intelligente Videoüberwachung: eine Handreichung, S. 20.
[361] Ebd. S. 20.
[362] Vgl. ebd. S. 20.
[363] Apelt/Möllers: Wie „intelligente" Videoüberwachung erforschen?, S. 589; Kees: Algorithmisches Panopticon, S. 30.
[364] Vgl. Kees: Algorithmisches Panopticon, S. 30.
[365] Vgl. Smoltczyk: Statement: Die Sicht der Aufsichtsbehörde in: Chancen und Risiken von Smart Cams im öffentlichen Raum, S. 132.
[366] Vgl. Kees: Algorithmisches Panopticon, S. 30.

II Gesellschaftliche Folgen des Einsatzes „intelligenter“ Systeme

Der Einsatz von VÜ hat nicht nur Einfluss auf die Wahrnehmung und Verhaltensweisen des Nutzers im überwachten Raum, sondern kann Auswirkungen auf die Gesellschaft im Ganzen entfalten. Insbesondere die Technik zur Verhaltenserkennung (Kapitel C) birgt erhebliche Gefahren. Der eingesetzte Algorithmus arbeitet immer nur so gut, wie er programmiert wurde. Es kann also nicht ausgeschlossen werden, dass dieser vielleicht falsch detektiert und/ oder falsch selektiert. Aber schon die Programmierung kann eine diskriminierende Wirkung hervorrufen. Es stellt sich die grundsätzliche Frage, wer definiert was konformes Verhalten ist und nach welchen Kriterien der Algorithmus Alarm schlägt. Um die sozialen Folgen relativ gering zu halten, sollte der Einsatz einer Verhaltenserkennung auf die in Kapitel C dargestellten Szenarien beschränkt bleiben, denn auch einfache Verhaltenserkennung kann zu Diskriminierung bis hin zur Exklusion führen.

„Soziale Exklusion bedeutet, dass Personen oder ganze Gruppen aufgrund bestimmter Merkmale (Alter, Ethnizität, Geschlecht, Religion etc.) aus bestimmten sozialen Prozessen, Ereignissen, Institutionen oder Räumen ausgeschlossen werden.“[367] Dies bedeutet für eine polizeiliche VÜ, dass die Entscheidungen des Überwachungspersonals, wer Ziel einer Beobachtung wird, durch Vorurteile behaftet sein kann und dass spezielle Gruppen häufiger detektiert werden als andere.[368] Diese Diskriminierung kann in verschärfter Form zum Ausschluss benannter Personen von Orten der Überwachungen führen, da sie immer mit Repressalien zu rechnen hätten. Neben der Diskriminierung besteht beim Einsatz von VÜ auch die Gefahr der Kriminalisierung des Einzelnen oder ganzer Gruppen.[369] Der Einsatz von intelligenten Videoüberwachungssystemen kann eine Verbesserung darstellen, da ein Algorithmus wertfrei arbeitet. Mögliche Treffer werden aufgrund statistischer Auffälligkeiten ausgelöst. Dies wiederum könnte aber auch die Diskriminierung verstärken, da einige Personengruppen statistisch häufiger für spezielle Delikte verant-

---

[367] Koch/Held u.a.: Intelligente Videoüberwachung: eine Handreichung, S. 20.
[368] Vgl. ebd. S. 20.
[369] Vgl. Kees: Algorithmisches Panopticon, S. 32.

wortlich sind. Bei einer automatisierten VÜ findet keine objektive Differenzierung des Verhaltens und persönlicher Charakteristika statt, sondern eine Kategorisierung. Hierin wird eindeutig eine diskriminierende Handlung gesehen.[370] Um dem entgegenzuwirken, bedarf es immer eines menschlichen Entscheiders für weitere Maßnahmen.[371]

Seit dem Ende des 20. Jahrhunderts setzte ein grundlegender Wandel der sozialen Kontrolle durch die Abkehr der Sicherheits- und Kriminalpolitik von ihren eigentlichen Aufgaben ein. „Staatliche Überwachung im klassischen Sinne diente vor allem der Beschaffung von Beweisen zum Nachweis der Schuld eines Täters oder zur Erkennung von Gefahren."[372] Heute bezieht sie sich nicht mehr auf einen konkreten Einzelfall, sondern ist zunehmend unabhängiger von Anlässen. Das drückt sich auch in einer Ausweitung des Gefahren- und Risikobegriffs aus und in der „deutlichen Tendenz zu einer immer weitergehenden Vorverlagerung der Strafbarkeit." [373] Videoüberwachung und insbesondere „intelligente Systeme" sind maßgeblich für die Entwicklung (mit-) verantwortlich. „So werden durch den Gesetzgeber zunehmend neue Gefährdungstatbestände geschaffen, um den Zugriff staatlicher Strafgewalt auch schon weit vor dem Eintritt einer Verletzung zu ermöglichen"[374]. Dies hat letztlich auch Auswirkungen auf die Arbeit der Sicherheitsbehörden. Die neue Kontroll- und Überwachungskultur resultiert aus Gewährleistungskompetenzen, die dem Staat die Beherrschbarkeit von möglichen Gefahren ermöglichen soll.[375]

Weitere gesellschaftliche Folgen könnten durch den Missbrauch der Technologie zu einer totalitären Überwachung führen oder durch das Abschöpfen sensibler Daten durch Unberechtigte entstehen.

---

[370] Vgl. Kees: Algorithmisches Panopticon, S. 32.
[371] Vgl. Vagts: Privatheit und Datenschutz in der intelligenten Überwachung, S. 69f.
[372] Singelnstein/Stolle: Von der sozialen Integration zur Sicherheit durch Kontrolle und Ausschluss in Surveillance Studies, S. 48.
[373] Vgl. ebd. S. 49.
[374] Heinrich: Zum heutigen Zustand der Kriminalpolitik in Deutschland, S. 5.
[375] Vgl. Zabel: Das Paradox der Prävention in: Der Staat und die Sicherheit, S. 55.

H Zusammenfassung und Ausblick

Im Rahmen dieser Arbeit ging es darum, eine technische Abgrenzung von konventioneller zu einer intelligenten Videoüberwachung vorzunehmen und dabei die unterschiedlichen Arten von automatisierten Analysemöglichkeiten vorzustellen. Dabei wurde festgestellt, dass es nicht *die* intelligente Videoüberwachung gibt. Vielmehr lassen sich darunter verschiedene Funktionen der Videoanalyse und des automatisierten Datenabgleichs in Echtzeit (Live) bzw. retrograd subsumieren. Die Bandbreite der technischen Möglichkeiten reicht von einer einfachen Objektdetektion, über die Verhaltens- und Gesichtserkennung bis zu einem automatisiertem Datenabgleich der extrahierten biometrischen Gesichtsmerkmale mit entsprechenden Datenbanken. Die Pauschalisierung der Begrifflichkeit „intelligente Videoüberwachung“ ist insofern nachteilig, da keine einheitliche Definition existiert und die verschiedenartig existierenden Verfahren für einen polizeilichen Einsatz unterschiedliche Wirkungen entfalten würden.

Obwohl seit dem letzten Test unter realen Einsatzbedingungen durch das BKA zum Einsatz einer biometrischen Gesichtserkennung über zehn Jahre vergangen sind und sich verschiedene zivile Forschungsprojekte dem Thema gewidmet haben, ist bis zum heutigen Tag keine entsprechende Technik/ Software im polizeilichen Einsatz. Eine Ausnahme bildet die automatisierte Kfz-Kennzeichenerfassung, da an diese geringere technische wie auch rechtliche Anforderungen gestellt werden. Für die Erkennung und Verarbeitung von physiologischen bzw. verhaltensbezogenen Merkmalen sind diese Anforderungen weitaus höher und dennoch stellten diese für die in der Arbeit dargestellten Projekte den Schwerpunkt der Forschungsarbeit dar, da man sich durch die Analyse dieser Merkmale eine effektivere Wirkungsweise der VÜ erhofft. Hierbei wurden die selbstdefinierten Ziele dieser Projekte erfüllt. Diese korrespondieren aber nicht immer mit den durch die Politik kommunizierten Erwartungen. Hiernach erhofft man sich durch den Einsatz intelligenter Systeme der VÜ eine deutliche Verbesserung zur Verhinderung von Straftaten, bei der Aufklärung von bereits eingetreten Rechtsgutsverletzungen und eine daraus resultierende Stärkung des (subjektiven) Sicherheitsgefühls in der Bevölkerung.

Gemessen an den drei Primärzielen lassen sich aufgrund des fehlenden Einsatzes entsprechender Systeme im öffentlichen Raum folgende Vermutungen ableiten:

1. VÜ als ein Instrument der situativen Kriminalprävention kann in einigen Fällen, in Abhängigkeit von Örtlichkeiten, Tätertypen und Delikten eine kriminalpräventive Wirkung entfalten. Studien haben gezeigt, dass die Einflussnahme dieses technischen Hilfsmittels geringer ausfällt, als die Erwartungen gemeinhin sind. Ausgehend vom heutigen Erkenntnisstand ist davon auszugehen, dass der Einsatz von Gesichtserkennungssoftware zumindest bei einem rational agierenden Täter eine größere Abschreckung entfalten kann. Die Verhinderung von Straftaten kann über die Einflussnahmen auf Verhaltensweisen von potenziellen Tätern und Opfern auch durch eine frühzeitige Intervention von Sicherheitskräften gewährleistet werden. Objektdetektion von zurückgelassenen und gefährlichen Gegenständen oder die biometrische Erkennung bekannter Straftäter und Gefährder sowie normabweichenden Verhaltens könnte dies ermöglichen. Intelligente Systeme der VÜ hätten zudem das Potenzial terroristische Bedrohungen - nicht durch Abschreckung der Täter - aber durch frühzeitige Detektion einer Gefährdungslage zu verhindern und würden so einen erheblichen Mehrwert zur konventionellen VÜ darstellen.

2. Durch die weite Verbreitung der konventionelle VÜ ist sie heute schon vielfach ein Hilfsmittel bei der Aufklärung von Straftaten, der Überführung von Tätern und dient als Beweismittel in Strafverfahren. Vielmals fehlt es nicht an Videoaufzeichnungen einer Tathandlung oder des Täters im Umfeld eines Tatortes, sondern an personellen und zeitlichen Ressourcen diese zeitnah gerichtsverwertbar auszuwerten. Die automatisierte Analysemöglichkeit in Verbindung mit einer Gesichtserkennungssoftware könnte diesen Prozess deutlich beschleunigen und VÜ dadurch wesentlich effizienter machen. Auch die Identifikation von unbekannten Straftätern könnte effektiver gestaltet werden und dabei mit weniger Grundrechtverletzungen für den Täter einhergehen als das strafprozessuale Mittel der Öffentlichkeitsfahndung.

3. Das Vertrauen und der Glaube in technische Hilfsmittel der Polizeibehörden ist in der Bevölkerung hoch. Doch vielmals ist Technik nicht in der Lage, die in sie gelegten Erwartungen zu erfüllen. Dies ist ein Grund, warum neue Technologien bei ihrer Einführung einen größeren Einfluss auf das subjektive Sicherheitsgefühl entfalten, welches im Laufe der Zeit nachlässt. So liegt die Vermutung nahe, dass die Einführung von intelligenten Systemen der VÜ anfänglich einen positiven Einfluss auf das subjektive Sicherheitsgefühl entfalten wird, aber mittel- und langfristig zu keiner nennenswerten Verbesserung beitragen wird. Das Sicherheitsgefühl wird durch viele Faktoren und persönliche Erfahrungen und Wahrnehmungen beeinflusst und lässt sich nicht exakt auf einen überwachten Raum beschränken. Vielmehr ist der Einsatz von VÜ im Allgemeinen und die Diskussion über den Einsatz intelligenter Systeme ein Ausdruck des Staates, etwas für die Sicherheit seiner Bürger zu tun und sie nehmen die Sorge um ihre Person und die Fürsorge wohlwollend zur Kenntnis.

Vereitelte Rechtsgutverletzungen, zeitnahe Ermittlungserfolge und rechtskräftige Verurteilungen aufgrund von Videomaterial als Beweismittel nehmen einen positiven Einfluss auf die drei primären Ziele der VÜ. Ein positiver Einfluss durch den möglichen Einsatz intelligenter Analyse- und Auswertungssysteme lässt sich zumindest vermuten.

Darüber hinaus werden die Reduzierung von Kosten für die Überwachung von Objekten und Räumen durch Personaleinsparungen und die Disziplinierung der Verhaltensweisen der Nutzer der beobachteten Räume als weitere Ziele der VÜ definiert. Auf beide Felder dürfte der Einsatz intelligenter Systeme einen größeren Einfluss entfalten, als die bisherige konventionelle VÜ. Die Stärke einer automatisierten Analyse und Auswertung liegt insbesondere in einer Zeit- und Personaleinsparung für die Ermittlungsbehörden bei der Auswertung großer Videomassedaten. Zudem dürfte der Einsatz von Algorithmen der Gesichts- und Verhaltenserkennung die Disziplinierung von Nutzern der überwachten Räume beeinflussen, da sie ihre Verhaltensweisen dahingehend anpassen, dass sie sich sozialkonform verhalten, um nicht in den Fokus der Überwachung zu geraten.

Die unterschiedlichen Möglichkeiten, welche unter dem Begriff der intelligenten VÜ subsumiert werden, greifen auch in unterschiedlicher Intensität in die Grundrechte der Betroffenen ein. Während es für den Einsatz eines Kfz-Kennzeichenerfassungsgerätes in einigen Landespolizeigesetzen bereits Ermächtigungsgrundlage gibt, fehlen diese für den Einsatz zur Erkennung von biometrischen bzw. verhaltensbezogenen Merkmalen gänzlich. Bei diesen Verfahren ist aber der größte Eingriff in individuelle Rechtsgüter der Betroffenen zu erwarten. Hier liegt es am Gesetzgeber, entsprechende Eingriffsbefugnisse für die Ermittlungsbehörden zu schaffen und dabei Eingriffsschwellen zu definieren, die den Einsatz entsprechender Systeme nicht zu einer ubiquitären Überwachung werden lassen. Gerade die intelligenten Systeme bieten die Chance, durch eine automatisierte Selektion, dass sich die VÜ zu einer freiheitsschützenden Überwachungstechnologie entwickeln könnte.

Die Akzeptanz der Bevölkerung gegenüber der konventionellen VÜ ist hoch und das scheint auch für den geplanten Einsatz von gesichts- und verhaltenserkennenden Algorithmen zuzutreffen und das obwohl keine merkliche Verbesserung im präventiven und repressiven Wirken dieser Technik empirisch nachgewiesen werden konnte. Zudem gehen mit der Etablierung entsprechender Systeme Risiken für den Einzelnen und die Gesellschaft einher, die vielmals bei der persönlichen Bewertung ausgeblendet werden. Die Gründe hierfür sind unterschiedlich und reichen von einem unbewussten Verdrängen hin zu einem aktiven Ausblenden, da man sich selbst weniger als „Opfer“ der Überwachung wahrnimmt. Die Akzeptanz könnte aber abnehmen, wenn die Falscherkennungsrate der Gesichts- und Verhaltenserkennung zu hoch ist. Werden unbescholtene Nutzer des videoüberwachten Raums fälschlicherweise identifiziert und weiteren Maßnahmen ausgesetzt, könnte der Glauben in die Funktionsweise einer solchen Technologie erschüttert werden.

Zudem sind die Risiken und Schäden eines Missbrauchs der gewonnen Daten im Vergleich zur konventionellen VÜ höher, da mehr Daten erhoben und gespeichert werden, als das nur das reine Videobild und die Qualität dieser personenbezogenen Daten weitaus höher liegt.

Die Videotechnik und -verfahren, die eine automatisierte Analyse und Auswertung ermöglichen, werden sich in der Zukunft weiterentwickeln. Sollte das Pilotprojekt „Sicherheitsbahnhof Berlin Südkreuz“ durch das verantwortliche Bundesministerium des Innern als Erfolg gewertet werden, so ist eine Einführung der Gesichts- und Verhaltenserkennung flächendeckend, „mindestens im Bereich des Bundesinnenministeriums, also bei Bahnhöfen und Flughäfen“[376] wahrscheinlich. Hierfür bedarf es je nach Art und Umfang der Einführung einer gesetzlichen Grundlage. Das Recht hat die Funktion den technologischen Fortschritt zu ermöglichen und dabei den Bürger vor der Technik zu schützen und dafür zu sorgen, dass sie verfassungs- und sozialverträglich ist und dabei durch die Einführung einer gesetzlichen Grundlage der Technik zu einer gesellschaftlichen Akzeptanz zu verhelfen.[377]

Recht muss dabei mit zwei grundlegenden Schwierigkeiten umgehen. Es wird in der Gegenwart geschaffen und soll auch in der Zukunft wirken und muss dabei mit Faktoren umgehen, die sich nur schwer vorhersagen lassen. So sind einige Wirkungsweisen und Risiken absehbar, aber es bleibt immer ein unbestimmter Rest an Nichtwissen und Unsicherheiten, dem das Recht begegnen muss. Aus heutiger Sicht würde eine Ermächtigungsgrundlage eine Technik erlauben und regulieren, die es als fertiges Produkt noch gar nicht gibt und die sich in Zukunft weiterentwickeln wird. Dies ist auch die zweite Schwierigkeit. Die technische Entwicklung wird immer schneller sein, als der Gesetzgeber reagieren kann.[378] Dies macht es notwendig ein Maß zu finden neue Verfahren der Videoüberwachung rechtlich zu ermöglichen, aber dabei den Rahmen der Einsatzmöglichkeiten weder zu weit, noch zu eng abzustecken.

---

[376] de Maizière: Pressekonferenz zu Zwischenergebnisse und Fehlerquoten der Gesichtserkennung am Pilotprojekt „Sicherheitsbahnhof Berlin Südkreuz“ am 20.12.2017, auf https://netzpolitik.org/2017/de-maiziere-plant-flaechendeckende-gesichtserkennung-trotz-hoher-fehlerquoten-am-suedkreuz/, abgerufen am 25.01.2018.
[377] Vgl. Boehme-Neßler: Schattenseiten in Chancen und Risiken von Smart Cams im öffentlichen Raum, S. 240f.
[378] Vgl. ebd. S. 242.

Es erscheint sinnvoll die technischen Möglichkeiten der Objektdetektion und der Gesichts- und Verhaltenserkennung zeitlich aufeinander folgend gesetzlich zu normieren und somit als kriminalpräventives Instrument und als Bestandteil der Kriminaltechnik einzuführen.

Im ersten Schritt sollte die reine Objektdetektion, ohne Personenbezug, zum Lokalisieren zurückgelassener Gegenstände im Bereich der kritischen Infrastruktur etabliert werden. Im zweiten Schritt kann dann die Gesichtserkennung eingeführt werden. Hierfür wäre eine gesetzliche Grundlage notwendig, diese muss nach ihrer Zielrichtung entweder präventiver oder repressiver Natur sein. Es bietet sich an, für die retrograde Auswertung von Videomassedaten die Gesichtserkennung eher zu normieren, da hier aufgrund der bereits eingetretenen Rechtsgutverletzungen, eine Prüfung der Eingriffsschwelle zum legitimen Einsatz dieser Technik einfacher gestaltet ist. Weiterhin werden in diesem Fall die Rechte unbeteiligter Dritter weniger tangiert. Zudem haben technische Defizite, wie die Falscherkennungsrate weniger Einfluss, da die zeitliche Dringlichkeit für Entscheidungen im Vergleich zur Live-Beobachtung weitestgehend entfällt.

Sollte sich die Technik der retrograden Gesichtserkennung bewährt haben kann über die Einführung einer flächendeckenden VÜ mit Live-Auswertung diskutiert werden. Diese stellt neben der Verhaltenserkennung den größten Eingriff in die Persönlichkeitsrechte der Nutzer des überwachten Raumes dar und würde im Falle eines Treffers (auch Fehlalarms) zu weiteren Maßnahmen, der agierenden Sicherheitskräfte und somit auch mit weiteren Eingriffen in die Rechte der Betroffenen einhergehen.

Die Verhaltenserkennung selbst beinhaltet einen komplexen Bereich an Einsatzmöglichkeiten. Das Erkennen einer liegenden, eventuell hilflosen Person, ist technisch realisierbar und stellt einen geringeren Eingriff in das Recht des Betroffenen dar, als ein Algorithmus der auf das Erkennen von abweichenden Verhalten, im Sinne einer gerade stattfindenden Tathandlung ausgerichtet ist. Fallbeispiele, wie das erstgenannte könnten nach erfolgreicher Erprobung zusammen mit der präventiven Gesichtserkennung eingeführt werden.

Quellenverzeichnis

Ackermann, Rolf/ **Clages**, Horst/ **Roll**, Holger: Handbuch der Kriminalistik: Kriminaltaktik für Praxis und Ausbildung, 4. Auflage, Richard Boorberg Verlag, Stuttgart, 2011.

Anstädt, Torsten/ **Keller**, Ivo/ **Lutz**, Harald: Intelligente Videoanalyse: Handbuch für die Praxis, Wiley-VCH Verlag, Weinheim, 2010.

Apelt, Maja/ **Möllers**, Norma: Wie „intelligente" Videoüberwachung erforschen? - Ein Resümee aus zehn Jahren Forschung zu Videoüberwachung in Zeitschrift für Außen- und Sicherheitspolitik, S. 585-590, 4/2011, Springer Verlag, Heidelberg, 2011.

Apple: Informationen zur fortschrittlichen Technologie von Face ID auf https://support.apple.com/de-de/HT208108, abgerufen am 24.11.2017.

Armitage, Rachel/ **Smyth**, Graham/ **Pease**, Ken: Burnley CCTV evaluation, S. 225-249, in: **Painter**, Kate/ **Tilley**, Nick (Hrsg.): Surveillance of Public Space: CCTV, Street Lighting and Crime Prevention, Crime Prevention Studies Vol. 10, New York, 1999.

Bartsch, Verena: Rechtsvergleichende Betrachtung präventiv-polizeilicher Videoüberwachungen öffentlich zugänglicher Orte in Deutschland und in den USA. (Schriften zum Internationalen Recht), Duncker & Humblot, Berlin, 2004.

Bergfink, Alexander Videoüberwachung im öffentlichen Personennahverkehr: Effektives Datenschutzmanagement bei einer Videoüberwachung in Bahnhöfen und Fahrzeugen des ÖPNV 2016, OlWIR Verlag, Edewecht, 2017.

Bergfink, Alexander: Videoüberwachung im ÖPNV in **Taeger**, Jürgen (Hrsg.): Chancen und Risiken von Smart Cams im öffentlichen Raum, Nomos Verlagsgesellschaft, Baden-Baden, 2017.

Bergmann, Lutz/ **Möhrle**, Roland/ **Herb**, Armin: Datenschutzrecht, 53. Ergänzungslieferung, Richard Boorberg Verlag; Stuttgart, 2017.

Berliner Morgenpost: Polizei sucht mit Foto nach U-Bahn-Schläger vom 01.11.2017, auf https://www.morgenpost.de/berlin/polizeibericht/article212407833/Polizei-sucht-mit-Foto-nach-U-Bahn-Schlaeger.html, abgerufen am 20.12.2017.

Biselli, Anna: „Projekt Sicherheitsbahnhof“: Intelligente Videoüberwachung am Berliner Südkreuz startet im Herbst vom 12.04.2017, auf https://netzpolitik.org/2017/projekt-sicherheitsbahnhof-intelligente-videoueberwachung-am-berliner-suedkreuz-startet-im-herbst/, abgerufen am 08.12.2017.

Boehme-Neßler, Volker: Schattenseiten. Warum Smart Cams im öffentlichen Raum ein Problem sind in **Taeger**, Jürgen (Hrsg.): Chancen und Risiken von Smart Cams im öffentlichen Raum, S. 235-267, Nomos Verlagsgesellschaft, Baden-Baden, 2017.

Brenneisen, Hartmut/ **Staack**, Dirk: Die Videobildübertragung nach allgemeinem Polizeirecht, in Datenschutz und Datensicherheit, S. 447-450, Springer Verlag, Heidelberg, 1999.

Bretthauer, Sebastian: Intelligente Videoüberwachung - Eine datenschutzrechtliche Analyse unter Berücksichtigung technischer Schutzmaßnahmen, Nomos Verlag, Frankfurt am Main, 2017.

Bücking, Hans-Jörg: Polizeiliche Videoüberwachung öffentlicher Räume, Duncker&Humblot GmbH, Berlin, 2007.

Bücking, Hans-Jörg/ **Kubera**, Thomas: „Eine digitale Streifenfahrt…“: Evaluation einer Videoüberwachung beim Polizeipräsidium Bielefeld, Schriftenreihe Polizei & Wissenschaft, Verlag für Polizeiwissenschaft, Frankfurt am Main, 2004.

Bull, Hans Peter: Fehlentwicklungen im Datenschutz am Beispiel der Videoüberwachung, in Juristen Zeitung, 72. Jahrgang, S. 797-807, Verlag C.H.BECK, München, 2017.

Büllesfeld, Dirk: Polizeiliche Videoüberwachung öffentlicher Straßen und Plätze zur Kriminalitätsvorsorge, Boorberg, Freiburg (Breisgau), 2002.

Bundesamt für Sicherheit in der Informationstechnik: Grundsätzliche Funktionsweise biometrischer Verfahren auf https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/Biometrie/AllgemeineEinfuehrung/einfuehrung.html, abgerufen am 06.12.2017.

Bundesministerium des Inneren: Sicherheitsbahnhof Berlin Südkreuz, Pressemitteilung vom 01.08.2017, auf https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2017/08/gesichtserkennungstechnik-bahnhof-suedkreuz.html, abgerufen am 23.11.2017.

Bundesministerium für Bildung und Forschung: Projektbeschreibung Flexibles, teilautomatisiertes Analysesystem zur Auswertung von Videomassendaten (FLORIDA), abgerufen am 11.12.2017.

Bundesministerium für Bildung und Forschung: Projektbeschreibung Kooperative Systemplattform für Videoupload, Bewertung, teilautomatisierte Analyse und Archivierung (PERFORMANCE), abgerufen am 12.12.2017.

Bundesministerium für Bildung und Forschung: Bewilligte Projekte aus der Bekanntmachung „Mustererkennung“, auf https://www.sifo.de/de/bewilligte-projekte-aus-der-bekanntmachung-mustererkennung-1771.html, abgerufen am 24.11.2017.

Bundesministerium für Verkehr, Innovation und Technologie: Produktbeschreibung FLORIDA, auf http://www.kiras.at/gefoerderte-projekte/detail/d/florida/, abgerufen am 15.12.2017.

Bundespolizei: Bundespolizei Jahresbericht 2016 auf https://www.bundespolizei.de/Web/DE/Service/Mediathek/Jahresberichte/jahresbericht_2016_file.pdf?__blob=publicationFile&v=2, abgerufen am 09.12.2017.

BÜNDNIS 90/DIE GRÜNEN: Zukunft wird aus Mut gemacht - Bundestagswahlprogramm 2017 auf https://www.gruene.de/fileadmin/user_upload/Dokumente/BUENDNIS_90_DIE_GRUENEN_Bundestagswahlprogramm_2017_barrierefrei.pdf, abgerufen am 15.11.2017.

Christlich Demokratische Union Deutschlands: Für ein Deutschland, in dem wir gut und gerne leben. - Regierungsprogramm 2017 – 2021 auf https://www.cdu.de/system/tdf/media/dokumente/170703regierungsprogramm2017.pdf?file=1&type=field_collection_item&id=9932, abgerufen am 15.11.2017.

Creifelds, Carl: Rechtswörterbuch, Verlag C.H. Beck, München, 20. Auflage, 2011.

Cohen, Lawrence E./ **Felson**, Marcus: Social Change and Crime Rate Trends: A Routine 1979 Activity Approach. in: American Sociological Review, 44, American Sociological Association, S. 588-608, 1979.

Die Bundesregierung der Bundesrepublik Deutschland: Einsätze von sogenannten Stillen SMS, WLAN-Catchern, IMSI-Catchern, Funkzellenabfragen sowie Software zur Bildersuche im ersten Halbjahr 2017 in Deutscher Bundestag Drucksache 1/13205, auf http://dipbt.bundestag.de/doc/btd/18/132/1813205.pdf, abgerufen am 08.12.2017.

Decker, Carsten: Muskat – Nicht nur ein Gewürz in Bundespolizei kompakt 03/2015.

Der Tagesspiegel: Berliner befürworten Ausbau der Videoüberwachung vom 30.01.2017 auf http://www.tagesspiegel.de/berlin/forsa-umfrage-berliner-befuerworten-ausbau-der-videoueberwachung/19324248.html, abgerufen am 11.11.2017.

Die Linke: Wahlprogramm der Partei DIE LINKE zur Bundestagswahl 2017 (Langfassung) auf https://www.die-linke.de/fileadmin/download/wahlen2017/wahlprogramm2017/die_linke_wahlprogramm_2017.pdf, abgerufen am 15.11.2017.

Dietrich, Dorothee: Wirksamkeit der polizeilichen Videoüberwachung – eine Analyse des Forschungsstandes, Kriminalistische Institut des Bundeskriminalamts, Berlin, 2015.

Dolderer, Michael: Verfassungsfragen der „Sicherheit durch Null-Toleranz" in Neue Zeitschrift für Verwaltungsrecht, Heft 2, 2011, S. 130-137, C.H.BECK, München, 2011.

Drewes, Michael/ **Malmberg**, Karl Magnus/ **Walter**, Bernd: Bundespolizeigesetz BPolG, 5. neu bearbeitete Auflage, Boorberg Verlag, Stuttgart, 2015.

Egbert, Simon/ **Paul**, Bettina: Zur Einführung in das Themenheft: Über den Mehrwert soziotechnischer Perspektiven für die Kriminologie in Kriminologisches Journal, Themenheft "Soziotechnische Perspektiven für die Kriminologie", 49. Jahrgang, 2017 Heft 2, Beltz-Juventa Verlag, Weinheim, 2017.

Eifler, Stefanie/ **Brandt,** Daniela: Videoüberwachung in Deutschland - Theorie und Praxis situationsbezogener Kriminalprävention, Monatsschrift für Kriminologie und Strafrechtsreform, S. 157 – 173, 88. Jahrgang, Heft 3 (Juni) 2005, Heymanns Verlag, Köln, 2005.

Eigenseer, Alex Elisabeth/ **Humer**, Stephan G./**Lederer**, Anna: Von der konventionellen zur intelligenten Videoüberwachung – Chancen und Risiken für Polizei und Gesellschaft, S. 147-158 in **Rüdiger,** T-G/ **Bayerl,** P.S. (Hrsg.): Digitale Polizeiarbeit, Springer Fachmedien, Wiesbaden, 2018.

Feltes, Thomas/ **Kudlacek**, Dominic/ **Ruch**, Andreas: Schlussbericht zum Verbundprojekt: Analyse von Personenbewegungen an Flughäfen mittels zeitlich rückwärts- und vorwärtsgerichteter Videodatenströme (APFel), auf https://www.sifo.de/de/apfel-analyse-von-personenbewegungen-an-flughaefen-mittels-zeitlich-rueckwaerts-und-1855.html, abgerufen am 08.12.2017.

Fillbrandt, Holger: Videobasiertes Multi-Personentracking in komplexen Innenräumen, Verlag Dr. Hut, München, 2007.

Frevel, Bernhard/ **Rinke**, Bernhard: Innere Sicherheit als Thema parteipolitischer Auseinandersetzung in Aus Politik und Zeitgeschichte: Innere Sicherheit, S. 4-10, Zeitschrift der Bundeszentrale für politische Bildung, Bonn, 2017.

Gaul, Thomas: Untersuchung der verfassungsrechtlichen Anforderungen an Videoüberwachungsmaßnahmen des Staates im öffentlichen Raum mit und ohne biometrische Erkennungsverfahren unter besonderer Berücksichtigung der hermeneutischen Erkenntnismethoden im Verfassungsrecht, Dissertation zur Erlangung der Würde eines doctor iuris der Juristischen Fakultät der Julius-Maximilians-Universität, Würzburg, 2007.

Geske, Katrin: Technisch-ethisches Gutachten im Zuge des Projekts „Multisensoriell gestützte Erfassung von Straftätern in Menschenmengen bei komplexen Einsatzlagen“, Universität Tübingen, 2017.

Glaeßner, Gert-Joachim: Sicherheit und Freiheit, in Aus Politik und Zeitgeschichte: Verwundbarkeit hochindustrieller Gesellschaften - Innere Sicherheit – Demokratie, Band 10-11/2002, Zeitschrift der Bundeszentrale für politische Bildung, Bonn, 2002.

Glatzner, Florian: Die staatliche Videoüberwachung des öffentlichen Raumes-Verlag Dr. Müller, Saarbrücken, 2008.

Grochwski, Maike: Aktuelle Praxis und Implikationen zur Identifikation von Attentätern – Polizeiliche Verhaltenserkennung mittels Behavioral Observation Analysis „BOA“, S. 23-25 in Bundespolizei kompakt, 39. Jahrgang, 05/2012.

Haberl, Tobias: Automatische Kennzeichenerkennung, auf http://www.sueddeutsche.de/auto/automatische-kennzeichenerkennung-wo-ihr-nummernschild-erfasst-wird-1.2188409, vom 23.10.2014, abgerufen am 09.01.2018.

Hamburger Abendblatt: Umfrage: Mehrheit der Deutschen für mehr Videoüberwachung vom 25.12.2016 auf https://www.abendblatt.de/politik/deutschland/article209084663/Umfrage-Mehrheit-der-Deutschen-fuer-mehr-Videoueberwachung.html, abgerufen am 11.11.2017.

Hegemann, Hendrik/ **Kahl**, Martin: Terrorismus und Terrorismusbekämpfung - Eine Einführung, Springer Fachmedien, Wiesbaden, 2018.

Heinrich, Bernd Zum heutigen Zustand der Kriminalpolitik in Deutschland in Kriminalpolitische Zeitschrift, 1/2017, S. 4-20, Deutsche Hochschule der Polizei, Münster, 2017.

Herdegen, Matthias in **Maunz**, Theodor/ **Dürig**, Günter: Grundgesetz, 81. Auflage 2017, C.H.BECK, München, 2017.

Held, Cornelius: Intelligente Videoüberwachung – Verfassungsrechtliche Vorgaben für den polizeilichen Einsatz, Schriften zum Öffentlichen Recht, Band 1282, Duncker & Humblot, Berlin, 2014.

Hella Aglaia: Produktbeschreibung Verkehrszeichenerkennung auf http://www.aglaia-gmbh.de/verkehrszeichenerkennung, abgerufen am 24.11.2017.

Herrmann, Daniel: Möglichkeiten und Grenzen des Einsatzes biometrischer Verfahren unter strafprozessualen Gesichtspunkten, Strafrecht in Forschung und Praxis, Band 272, Verlag Dr. Kovač, Hamburg, 2013.

Herrmann, Dieter: Kriminalitätstheorien, auf http://www.krimlex.de/artikel.php?BUCHSTABE=&KL_ID=108, abgerufen am 19.12.2017.

Hessisches Landeskriminalamt: Handlungsempfehlung für die Errichtung und den Betrieb von Videoüberwachungsanlagen im öffentlichen Raum auf https://www.polizei.hessen.de/File/2017-handlungsempfehlung-video-www_1.pdf, Stand Juli 2017, abgerufen am 20.12.2017.

Hoffmann, Jonas: Kombination von Inertialsensoren und GPS zur Navigation, Freie Universität, Berlin, 2010.

Hornung, Gerrit/ **Desoi**, Monika: "Smart Cameras" und automatische Verhaltensanalyse in Kommunikation & Recht, Heft 03/2011, S. 153, dfv Mediengruppe, Frankfurt am Main, 2011.

Hornung, Gerrit/ **Schindler**, Stephan: Das biometrische Auge der Polizei in Zeitschrift für Datenschutz 5/2017, S. 203-208, Verlag C.H.BECK, München, 2017.

Humer, Stephan G.: Abschlussbericht (öffentliche Version) Multi-Biometriebasierte Forensische Personensuche in Lichtbild- und Videomassendaten: Akronym: MisPel: Teilvorhaben: Sozialwissenschaftliche Begleitforschung (MisPel-S) auf https://www.tib.eu/de/suchen/id/TIBKAT%3A865668353/Multi-Biometriebasierte-Forensische-Personensuche/?tx_tibsearch_search%5Bsearchspace%5D=tn, abgerufen am 02.12.2017.

Hummelsheim-Doss, Dina: Objektive und subjektive Sicherheit in Deutschland in Aus Politik und Zeitgeschichte: Innere Sicherheit, S. 34-39, Zeitschrift der Bundeszentrale für politische Bildung, Bonn, 2017.

Jain, A.K./ **Bolle**, Ruud M./ **Pankanti**, Sharath: Biometrics - Personal Identification in Networked Society, Springer-Verlag US, 2006.

Karrer-Gauß, Katja: Prospektive Bewertung von Systemen zur Müdigkeitserkennung - Ableitung von Gestaltungsempfehlungen zur Vermeidung von Risikokompensation aus empirischen Untersuchungen, auf https://depositonce.tu-berlin.de/handle/11303/3482, 2012, abgerufen am 24.11.2017.

Kilchling, Michael/ **Kenzel**, Brigitte: Recht und Praxis der anlassbezogenen automatischen Kennzeichenfahndung, Verkehrsdatenabfrage und Mobilfunkortung zur Gefahrenabwehr in Brandenburg - Wissenschaftliche Begleitforschung zu den §§ 33b Abs. 3, Abs. 6 Satz 2 und 36a BbgPolG, Gutachten der kriminologischen Abteilung des Max-Planck-Instituts für ausländisches und internationales Strafrecht, im Auftrag des Brandenburgischen Ministeriums des Innern, Freiburg im Breisgau, 2011.

Kipp, Almut: „Alles normal" – Nach G20-Krawallen wieder Alltag im Schanzenviertel, 06.08.2017 auf https://www.shz.de/regionales/hamburg/g20-gipfel/alles-nor, mal-nach-g20-krawallen-wieder-alltag-im-schanzenviertel-id17495381.html, abgerufen am 15.12.2017.

Kenzel, Brigitte: Die automatische Kennzeichenfahndung: Eine neue Überwachungsmaßnahme an der Schnittstelle zwischen präventivem und repressivem Einsatz, Verlag Dr. Kovac, Hamburg, 2013.

Kees, Benjamin J.: Algorithmisches Panopticon: Identifikation gesellschaftlicher Probleme automatisierter Videoüberwachung, Verlagshaus Monsenstein und Vannerdat OHG, Münster, 2015.

Knape, Michael: Videogeräteeinsatz – ein Plädoyer für den Schutz durch Videoüberwachung, Die POLIZEI, Ausgabe 7, S. 207-211, Carl Heymanns Verlag, Köln, 2017.

Koch, Heiner/ **Held**, Cornelius/ **Matzner**, Tobias, u.a.: Intelligente Videoüberwachung: eine Handreichung, Materialien zur Ethik in den Wissenschaften Band 11, Internationalen Zentrum für Ethik in den Wissenschaften (IZEW), Eberhard-Karls-Universität, Tübingen, 2015.

Kudlacek, Dominic: Akzeptanz von Videoüberwachung - Eine sozialwissenschaftliche Untersuchung technischer Sicherheitsmaßnahmen, Springer Fachmedien, Wiesbaden, 2015.

Labudde, Dirk: Biometrie und die Analyse digitalisierter Spuren in **Labudde**, Dirk/ **Spranger**, Michael (Hrsg.): Forensik in der digitalen Welt Moderne Methoden der forensischen Fallarbeit in der digitalen und digitalisierten realen Welt, S. 25-58, Springer-Verlag, Berlin, 2017.

Lee, Morris/ **Reirach**, Boris: Einsatz von Body Cams bei privaten Sicherheitsdiensten in **Taeger**, Jürgen (Hrsg.): Chancen und Risiken von Smart Cams im öffentlichen Raum, S. 209-225, Nomos Verlagsgesellschaft, Baden-Baden, 2017.

Lingg, Carmen: Videoüberwachung im öffentlichen Raum – eine Analyse kriminologischer Aspekte mit Blick auf die Videoüberwachung auf dem Bahnhofsplatz in der Stadt Luzern, in **Schwarzenegger**, Christian/ **Nägeli**, Rolf (Hrsg.): 3. Zürcher Präventionsforum – Videoüberwachung als Prävention?, S. 13-105, Schulthess Juristische Medien AG, Zürich, Basel, Genf, 2010.

Maximini, Dominique: Polizeiliche Videoüberwachung öffentlicher Straßen und Plätze zur Kriminalitätsprävention, Verlag Alma Mater, Saarbrücken, 2011.

Meuth, Lotte: Zulässigkeit von Identitätsfeststellungen mittels biometrischer Systeme durch öffentliche Stellen, Beiträge zum Informationsrecht Band 17, Duncker & Humbold, Berlin, 2006.

Möllers, Martin: Wörterbuch der Polizei, 2. Neu bearbeitete und erweiterte Auflage, Verlag C.H.BECK, München, 2010.

Monroy, Matthias: BKA schließt Probelauf zur Gesichtserkennung ab, auf https://netzpolitik.org/2017/bka-schliesst-probelauf-zur-gesichtserkennung-ab/, Artikel vom 10.08.2017, abgerufen am 08.12.2017.

Monroy, Matthias: G20-Gipfel: Polizei durchsucht zehntausende Dateien mit Gesichtserkennungssoftware, auf https://netzpolitik.org/2017/g20-gipfel-polizei-durchsucht-zehntausende-dateien-mit-software-zur-gesichtserkennung/, Artikel vom 28.09.2017, abgerufen am 12.12.2017.

Müller, Claudia: Mehr Kameras für mehr Sicherheit? in Kriminalistik 5/2017, S. 306-310, C.F. Müller, München, 2017.

Müller, Lucien: Videoüberwachung in öffentlich zugänglichen Räumen - insbesondere zur Verhütung und Ahndung von Straftaten, Nomos Verlag, Baden-Baden, 2012.

Ott, Florian Philipp: Vorbeugende Überwachung. Über Voraussetzungen für, Formen von und Erfahrungen mit präventiver Videoüberwachung im kommunalen Bereich, in: **Ott**, Florian Philipp/ **Ackerschott**, Stephan/ **Müller**, Nico: Kameras gegen Gewalt. Wie effektiv ist die öffentliche Videoüberwachung?, ScienceFactory, Norderstedt, 2013.

Petri, Thomas in **Lisken**, Hans/ **Denninger**, Erhard (Hrsg.): Handbuch des Polizeirechts, 5. Aufl., C.H.BECK, München, 2012.

Reimer, Helmut: Biometrische Identifikation – Eine aussichtsreiche Inovation, S. 1-25 in **Behrens**, Michael/ **Roth**, Richard (Hrsg.): Biometrische Identifikation – Grundlagen, Verfahren, Perspektiven, Verlag Vieweg, Braunschweig/Wiesbaden, 2001.

Reuband, Karl-Heinz: Kriminalitätsfurcht - Erscheinungsformen, Trends und soziale Determinanten in **Lange**, Hans-Jürgen/ **Ohly**, H. Peter/ **Reichertz**, Jo (Hrsg.): Auf der Suche nach neuer Sicherheit - Fakten, Theorien und Folgen, VS Verlag für Sozialwissenschaften, Wiesbaden, 2008.

Reuter, Markus: Zwei Drittel der Deutschen schätzen Kriminalitätsentwicklung falsch ein, Artikel vom 03.11.2016, auf https://netzpolitik.org/2016/repraesentative-umfrage-zwei-drittel-der-deutschen-schaetzen-kriminalitaetsentwicklung-falsch-ein/, abgerufen am 04.01.2018.

Roßnagel, Alexander/ **Desoi**, Monika/ **Hornung**, Gerrit: Gestufte Kontrolle bei Videoüberwachungsanlagen - Ein Drei-Stufen-Modell als Vorschlag zur grundrechtsschonenden Gestaltung in Datenschutz und Datensicherheit 10 / 2011, S. 694-701, Springer Verlag, Heidelberg, 2011.

Rothmann, Robert: Sicherheitsgefühl durch Videoüberwachung? - Argumentative Paradoxien und empirische Widersprüche in der Verbreitung einer sicherheitspolitischen Maßnahme, in Neue Kriminalpolitik Jg. 22, 2010, Nr. 3, S. 103-107, Nomos Verlagsgesellschaft, Baden-Baden, 2010.

Schäufele, Fabia: Profiling zwischen sozialer Praxis und technischer Prägung - Ein Vergleich von Flughafensicherheit und Credit-Scoring, Springer Fachmedien, Wiesbaden, 2017.

Schewe, Christoph: Subjektives Sicherheitsgefühl, in **Lange**, Hans-Jürgen (Hrsg.): Wörterbuch zur Inneren Sicherheit, S. 322-325, VS Verlag für Sozialwissenschaften, Wiesbaden, 2006.

Schieder, S. A.: Die automatisierte Erkennung amtlicher Kfz-Kennzeichen als polizeiliche Maßnahme, in: NVwZ 2004, Heft 7, S. 778-788, Verlag C.H.BECK, München, 2014.

Schnabel, Christoph: Die polizeiliche Videoüberwachung öffentlicher Orte in Niedersachen, in Datenschutz und Datensicherheit 12 / 2011, S. 879-883, Springer Verlag, Heidelberg, 2011.

Schulte, Thomas: Die Silvesternacht 2015/16 in Köln - Darstellung der Ermittlungen der EG Neujahr (Teil 3), in der kriminalist 6/2017, dbb Verlag GmbH, Berlin, 2017.

Schulz, André: Videoüberwachung: Mehr Kameras = Mehr Sicherheit? in der kriminalist 1-2/2017, dbb Verlag GmbH, Berlin, 2017.

Schwind, Hans-Dieter: Kriminologie: Eine praxisorientierte Einführung mit Beispielen (Grundlagen der Kriminalistik, Band 28), 22. neubearbeitete und ergänzte Auflage, Kriminalistik Verlagsgruppe, Heidelberg, u.a., 2013.

Simitis, Spiros (Hrsg.): Bundesdatenschutzgesetz, (zitiert als *Bearbeiter*, in: Simitis), 8., neu bearbeitete Auflage, Nomos Verlag, Baden-Baden, 2014.

Singelnstein, Tobias/ **Stolle**, Peer: Von der sozialen Integration zur Sicherheit durch Kontrolle und Ausschluss in **Zurawski**, Nils (Hrsg.): Surveillance Studies – Perspektiven eines Forschungsfeldes, S. 47-66, Verlag Barbara Budrich, Opladen & Farmington Hills, 2007.

Smoltczyk, Maja: Statement: Die Sicht der Aufsichtsbehörde in **Taeger**, Jürgen (Hrsg): Chancen und Risiken von Smart Cams im öffentlichen Raum, S. 129-140, Nomos Verlagsgesellschaft, Baden-Baden, 2017.

Starnecker, Tobias: Videoüberwachung zur Risikovorsorge - Body-Cam zur Eigensicherung und Dashcam zur Beweissicherung – Eine verfassungs- und datenschutzrechtliche Analyse, Duncker & Humbold, Berlin, 2017.

Stettner, Elisa: Sicherheit am Bahnhof: Überwachungsmaßnahmen zur Abwehr terroristischer Anschläge, Duncker & Humblot, Berlin, 2017.

Stiefelhagen, Rainer: Abschlussbericht für das BMBF-Projekt MisPel, auf https://www.tib.eu/de/suchen/id/TIBKAT%3A853198942/Abschlussbericht-f%C3%BCr-das-BMBF-Projekt-MisPel-Multi/, Karlsruhe, 2015, abgerufen am 08.12.2017.

Stolle, Peer: Situative Kriminalprävention: Konzept, Empirie, Bewertung: Exemplifiziert an der Videoüberwachung öffentlicher Orte, LIT Verlag, Berlin, 2015.

Tillich, Karin: Polizeiliche Videobeobachtung öffentlich zugänglicher Straßen und Plätze in München und Barcelona – Ein Städtevergleich, Felix-Verlag, Holzkirchen, 2014.

Vagts, Hauke-Hendrik: Privatheit und Datenschutz in der intelligenten Überwachung: Ein datenschutzgewährendes System, entworfen nach dem „Privacy by Design" Prinzip, Kit Scientific Publishing, Karlsruhe, 2013.

Videmo Intelligente Videoanalyse: Produktbeschreibung Videmo 360 auf http://videmo.de/produkte/videmo360/, abgerufen am 15.12.2017.

Voß, Axel: Videoüberwachung im öffentlichen Raum auf http://www.krimlex.de/artikel.php?BUCHSTABE=V&KL_ID=225, abgerufen am 24.11.2017.

Weber, Frank: Gesichtserkennung, S. 105-128 25 in **Behrens**, Michael/ **Roth**, Richard (Hrsg.): Biometrische Identifikation – Grundlagen, Verfahren, Perspektiven, Verlag Vieweg, Braunschweig/ Wiesbaden, 2001.

Welsh, Brandon C./ **Farrington**, David P.: Crime Prevention Effects of Closed Circuit Television: a Systematic Review, Home Office research, Development and Statistics Directorate, 2002.

Wissenschaftlicher Dienst des Deutschen Bundestages: Sachstand zur Legaldefinition des Begriffes „Gefährder" auf https://www.bundestag.de/blob/503066/8755d9ab3e2051bfa76cc514be96041f/wd-3-046-17-pdf-data.pdf, abgerufen am 07.01.2018.

Wolkenstein, Andreas F.X.: Intelligente Videoüberwachung aus ethischer Perspektive in forum kriminalprävention 3/2011, Stiftung Deutsches Forum für Kriminalprävention (DFK), Bonn, 2011.

Würtenberger, Thomas: Rechtswissenschaftliche Begleitforschung zur intelligenten Videoüberwachung, Manuskript, Freiburg, 2012.

Zabel, Benno: Das Paradox der Prävention Über ein Versprechen des Rechts und seine Folgen, in **Puschke**, Jens**/ Singelnstein**, Tobias (Hrsg.): Der Staat und die Sicherheitsgesellschaft, Springer Fachmedien, Wiesbaden, 2018.

Zeit online: Überwachungskamera liefert Hinweis auf Attentäter vom 17.04.2013 abgerufen am 11.12.2017.

Zurawski, Nils: Raum – Weltbild – Kontrolle, Raumvorstellungen als Grundlage gesellschaftlicher Ordnung und ihrer Überwachung, Budrich UniPress Ltd., Opladen • Berlin • Toronto, 2014.

Zurawski, Nils: Videoüberwachung. Praktische Überlegungen zu einer allgegenwärtigen Technologie, in: **Bisky**, Lothar/ **Kriese**, Konstanze/ **Scheele**, Jürgen (Hrsg.): Medien – Macht – Demokratie. Neue Perspektiven, Reihe: Texte/Rosa-Luxemburg-Stiftung, Bd. 54, Karl Dietz Verlag, Berlin, 2009.

Rechtsquellenverzeichnis

AG Hannover, Urteil vom 23.04.2015 - 174 Geschäftszeichen 434/15, „Öffentlichkeitsfahndung, Voraussetzung“, 2015.

BGBl I 2017 Nr. 23, S. 968 ff: Gesetz zur Änderung des Bundesdatenschutzgesetzes – Erhöhung der Sicherheit in öffentlich zugänglichen großflächigen Anlagen und im öffentlichen Personenverkehr durch optisch-elektronische Einrichtungen (Videoüberwachungsverbesserungsgesetz) vom 28. April 2017.

BGH, Urteil vom 17.12.1998 Az. 1 StR 156/98, „Polygraphentest als Beweismittel“, 1998.

BT-Drucksache 18/10941: Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes – Erhöhung der Sicherheit in öffentlich zugänglichen großflächigen Anlagen und im öffentlichen Personenverkehr durch optisch-elektronische Einrichtungen (Videoüberwachungsverbesserungsgesetz) vom 23.01.2017.

Bundesdatenschutzgesetz (BDSG) in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), das zuletzt durch Artikel 10 Absatz 2 des Gesetzes vom 31. Oktober 2017 (BGBl. I S. 3618) geändert worden ist.

BVerfG, Entscheidung vom 19.12.1951 - 1 BvR 220/51, „Deklaration der Grundrechte als Abwehrrechte“, 1951.

BVerfG, Beschluss vom 04.04.2006 Az. 1 BvR 518/02, „präventive polizeiliche Rasterfahndung“, 2006.

BVerfG, Beschluss der 1. Kammer des Ersten Senats vom 23. Februar 2007 - 1 BvR 2368/06 -, „Videoüberwachung“, 2007.

BVerfG, Urteil des Ersten Senats vom 11. März 2008, - 1 BvR 2074/05 - Rn. (1-185), „automatisierte Erfassung von Kraftfahrzeugkennzeichen“, 2008.

BVerwG, Urteil vom 22.10.2014 - 6 C 7.13: Einsatz einer Einrichtung der automatisierten Erfassung von Kraftfahrzeugkennzeichen und deren Abgleich mit Fahndungsdatenbeständen, 2014.

Gesetz über die Aufgaben und Befugnisse der Bayerischen Staatlichen Polizei (Polizeiaufgabengesetz – PAG) in der Fassung der Bekanntmachung vom 14. September 1990 (GVBl. S. 397, BayRS 2012-1-1-I), das zuletzt durch § 1 des Gesetzes vom 24. Juli 2017 (GVBl. S. 388) geändert worden ist.

Gesetz über die Aufgaben, Befugnisse, Organisation und Zuständigkeit der Polizei im Land Brandenburg (Brandenburgisches Polizeigesetz - BbgPolG) vom 19. März 1996 (GVBl.I/96, [Nr. 07], S.74), zuletzt geändert durch Artikel 14 des Gesetzes vom 25. Januar 2016 (GVBl.I/16, [Nr. 5]).

Gesetz über die Bundespolizei (Bundespolizeigesetz - BPolG), Artikel 1 Geltung vom 19.10.1994 BGBl. I S. 2978, 2979; zuletzt geändert durch Artikel 1 Geltung vom 05.05.2017 BGBl. I S. 1066.

Gesetz über die Datenverarbeitung der Polizei vom 2. Mai 1991 HmbGVBl. 1991, S. 187, letzte berücksichtigte Änderung: § 4 geändert durch Artikel 1 des Gesetzes vom 8. Dezember 2016 (HmbGVBl. S. 514).

Gesetz über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisgesetz - PAuswG) vom 18. Juni 2009 (BGBl. I S. 1346), das zuletzt durch Artikel 4 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2745) geändert worden ist.

Hessisches Gesetz über die öffentliche Sicherheit und Ordnung (HSOG) in der Fassung der Bekanntmachung vom 14. Januar 2005 (GVBl. I S. 14), zuletzt geändert durch Artikel 2 des Gesetzes vom 4. Mai 2017 (GVBl. S. 66).

Oberverwaltungsgericht Lüneburg - 11 LC 114/13-: Installation von Videokameras zur Überwachung öffentlicher Bereiche eines Bürogebäudes zur Wahrnehmung des Hausrechts und zur Verhinderung weiterer Straftaten zulässig, ZD 2014, S. 636, Urteil vom 17.09.2014.

Strafprozeßordnung, in der Fassung der Bekanntmachung vom 07.04.1987 (BGBl. I S. 1074, S. 1319) zuletzt geändert durch Gesetz vom 30.10.2017 (BGBl. I S. 3618) mit Wirkung vom 09.11.2017.

Ich versichere hiermit, dass ich die vorstehende Arbeit selbständig angefertigt habe und keine anderen als die angegebenen und bei Zitaten kenntlich gemachten Quellen und Hilfsmittel benutzt habe. Die Masterarbeit ist nicht anderweitig als Prüfungsleistung verwendet worden.

Christoph Sehrt